VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2019 Jan Klečka

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

AUTENTIZACE POMOCÍ PRVKŮ RFID
AUTHENTICATION WITH RFID TAGS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Jan Klečka**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Lukáš Malina, Ph.D.**
SUPERVISOR

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní obor **Informační bezpečnost**
Ústav telekomunikací

Student: Jan Klečka ***ID:*** 195811
Ročník: 3 ***Akademický rok:*** 2018/19

NÁZEV TÉMATU:

Autentizace pomocí prvků RFID

POKYNY PRO VYPRACOVÁNÍ:

Téma práce je zaměřeno na moderní autentizační a identifikační systémy. V rámci práce student srovná současné protokoly a řešení pro autentizaci a identifikaci, které využívají i RFID prvky. Dále budou srovnány možnosti aktivních a pasivních RFID prvků. Dále bude provedeno měření parametrů RFID prvků a měření jejich výkonu při výpočtu základních kryptografických algoritmů v případě aktivních prvků. Výstupem bakalářské práce bude verifikační implementace autentizačního protokolu využívající i RFID prvky.

DOPORUČENÁ LITERATURA:

[1] FINKENZELLER, Klaus. RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication. John Wiley & Sons, 2010.

[2] JUELS, Ari. RFID security and privacy: A research survey. IEEE journal on selected areas in communications, 2006, 24.2: 381-394.

Termín zadání: 1.2.2019 ***Termín odevzdání:*** 27.5.2019

Vedoucí práce: Ing. Lukáš Malina, Ph.D.
Konzultant:

prof. Ing. Jiří Mišurec, CSc.
předseda oborové rady

ABSTRAKT

Bakalářská práce se zabývá problematikou RFID prvků autentizačních systémů využívající prvky RFID a čipové karty. Jsou popsány základní rozdíly mezi aktivními a pasivními RFID prvky. Jsou popsány základní útoky, jakými se dá ohrozit komunikace mezi čtečkou a RFID zařízením v bezdrátovém prostředí. V práci je zahrnuto měření jednotlivých pasivních RFID tagů. Výsledky měření jsou zaznamenány pomocí tabulek a grafů. Hlavní cíl práce se zaměřuje na realizaci autentizačního protokolu, který je určen pro procesorové karty. Díky procesoru zde můžou být nasazeny protokoly využívající kryptografii, kde je vyžadován určitý výpočetní výkon. S využitím procesoru je možné zajistit bezpečný přenos dat a autentizaci. Práce popisuje 2 návrhy protokolů, které byly modifikovány pro BasicCard prostředí. V prvním schématu je představena autentizace klienta vůči terminálu, využívající zabezpečený přenos dat pomocí AES 256 bit a ověřovatel je strana terminálu. Ve druhém schématu je strana karty jako ověřovatel, kde karta generuje takové údaje, aby mohla ověřit, že druhá strana je schopná se autentizovat.

KLÍČOVÁ SLOVA

RFID, aktivní a pasivní tagy, identifikační systémy, kolize v RFID, bezpečnost, frekvence v RFID, autentizační protokol.

ABSTRACT

The bachaleror thesis deals with issue of RFID elements and authentication systems used by elements of RFID and chip cards. The basic differences between active and passive RIFD tags are decsribed. The thesis describes basic attacks which can threat communication between reader and RFID device in wireless comunication. In the thessis is included measuring of passive RFID tags. Results of the measurement are presented by tables and graphs. Main goal of this thesis aims at the implementation of the authentication protocol which is mainly for processor cards. Because of the processor we can use cryptography where is neccessary computing power. We can ensure secure data transfer and authentication. The thesis describes 2 schemes of one authentication protocol, which were modificated for BasicCard Enviroment. In the first scheme client(card) authenticate to the terminal using secure AES 256 bit data transfer and verifier is the terminal side. Data which needs to be exchanged is secured by AES 256 bit. In the second scheme the card side is a verifier and the card generated such data to verify that the other party is able to authenticate.

KEYWORDS

RFID, active and passive tags, identification systems, collision in RFID, security, frequency in RFID, authentication protocol.

KLEČKA, Jan. *Autentizace pomocí prvků RFID*. Brno, 2019, 57 s. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: prof. Ing. Lukáš Malina, CSc.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Autentizace pomocí prvků RFID“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autora

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu diplomové práce panu Ing. Lukáši Malinovi, Ph.D. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Brno ....

podpis autora

Faculty of Electrical Engineering
and Communication
Brno University of Technology
Purkynova 118, CZ-61200 Brno
Czech Republic

http://www.six.feec.vutbr.cz

PODĚKOVÁNÍ

Výzkum popsaný v této bakalářské práci byl realizován v laboratořích podpořených z projektu SIX; registrační číslo CZ.1.05/2.1.00/03.0072, operační program Výzkum a vývoj pro inovace.

Brno ....

podpis autora

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

OP Výzkum a vývoj
pro inovace

Obsah

Seznam obrázků

Seznam tabulek

Úvod

V dnešní době, kdy je většina identifikačních systému systému automatizována, se hledají způsoby, jak veškerou identifikaci usnadnit nebo automatizovat. Čárové kódy jsou typickým zástupcem, pomocí kterých se identifikují jednotlivé objekty. Nevýhodou je malá paměť a neschopnost přeprogramovat tyto kódy.

Modernější nástupce čárových kódů je technologie zvaná RFID (Radio freqeuncy identifikator). Technologie, která slouží pro automatické identifikování osob, zvířat a věcí. Technicky nejlepší řešení pro uložení a identifikaci je vložit data na elektronický čip, který bude identifikovatelný na určité vzdálenosti, podobné zařízení jako jsou platební karty. Přenos probíhá pomocí bezdrátového prostředí. RFID technologie je využívána v systémech, kde je potřeba rychlá identifikace a není možné skenovat každý čárový kód zvlášť.

Existuje způsob přenosu dat, který přenáší data stejně jako Wi–Fi. Prvky umožňující tento přenos byly nazvány RFID, kde se data přenáší bezdrátově a energie dodána ke zpracování a odesílaní dat na straně identifikovatelného předmětu nebo–li tagů vzniká působením elektromagnetického pole.

V práci je popsán úvod do RFID a představeny systémy, kde se RFID prvky mohou uplatnit. Vysvětlena základní problematika kolizí v RFID, které mohou nastat při výskytu více tagů v oblasti čtecí zóny čtečky a jejich řešení. V práci je ilustrován model útoků, které mohou hrozit RFID zařízení, riziko napadení přenosu signálu a odposlechu dat, který roste při přenosu bezdrátovým prostředím. Jsou zde představeny mechanismy, na kterých dále stojí identifikace a autentizace v RFID systémech. Dále práce popisuje systém Roger, který slouží pro měření UHF tagů.

Praktická část této práce popisuje protokol pro autentizaci s využitím na kartách s procesorem. Je zde využit Diffie–Helman protokol pro výměnu veřejných klíčů a následného vypočítání klíče pro AES 256 bit.

1 Úvod do autentizace a identifikace založené na RFID

Před samotným popisem RFID technologie je nezbytné definovat základní pojmy, které jsou spojené s bezpečnostní. Následující pojmy popsané v kapitole (1.1) popisují cíle kryptografie.

1.1 Základní pojmy

Integrita dat

Zamezení neoprávněné modifikace dat jako jsou: vložení nových dat, smazání určité části dat a další neoprávněné manipulace s daty.

Důvěrnost

Hlavní účel důvěrnosti je udržet obsah zprávy v tajnosti, hlavní cíl kryptografie.

Autentizace

Prokazování totožnosti. Ověřujeme, že ten s kým komunikujeme, je opravdu ten, s kterým chceme komunikovat. Může probíhat na základě hesla, vlastnictví předmětu a biometrické informace.

Autorizace

Přiděluje jednotlivým subjektům oprávnění.

Nepopíratelnost

Jistota, že autor nemůže popřít původ zprávy. Více o popisech služeb lze najít v [21].

1.2 Popis základních pojmů a představení technologie RFID

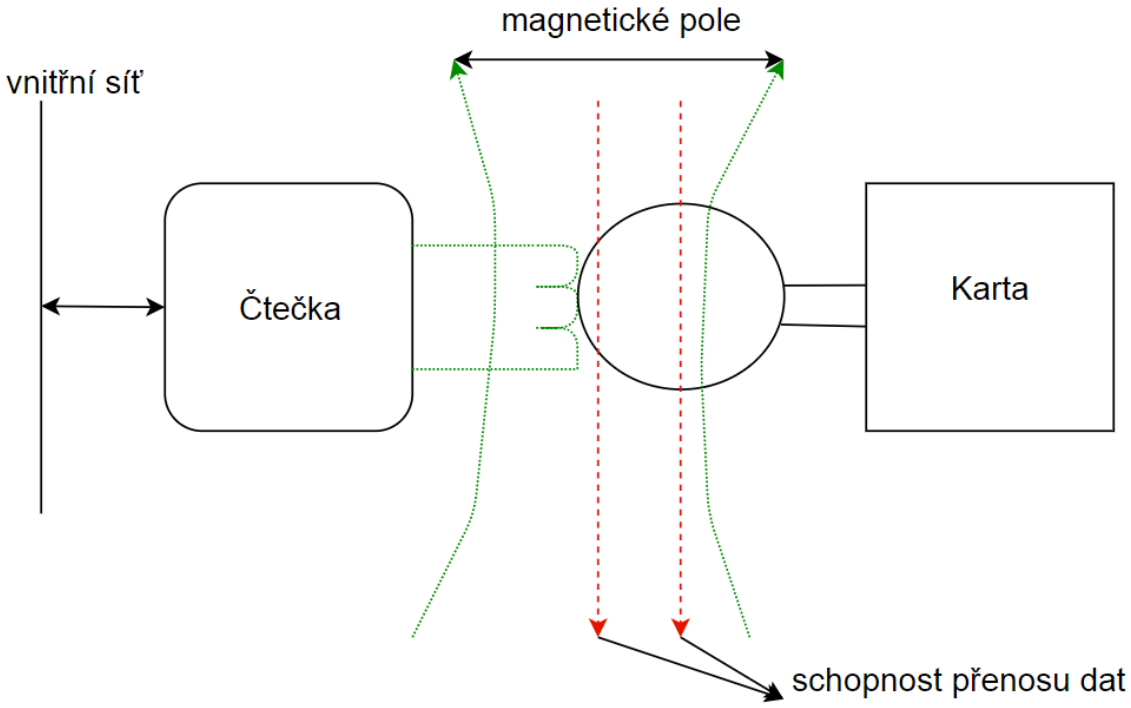
U RFID technologie jsou data uložená na elektronickém zařízení. Energie potřebná ke komunikace mezi nosičem a čtečkou je vytvořena magnetickým nebo elektromagnetickým polem.

Technologie slouží pro automatické detekování objektů a osob. V principu se technologie skládá pouze z RFID tagu, antény. RFID tag je mikročip, který slouží k bezdrátovému přenosu dat pomocí antény. Mikročip sám o sobě má velikosti kolem 0,4 mm^2. Anténa je nezbytnou součástí RFID tagu pro přijetí signálu a indukování napětí, které je nezbytné pro funkci tagu obr. (1.1).

Tag je mikročip umístěný na objektu a obsahuje unikátní identifikační číslo. Anténa slouží k příjmu elektromagnetického signálu. V důsledku elektromagnetického signálu dojde k vybuzení energie, sloužící pro předání EPC hodnoty u nejjednodušších RFID zařízení.[2]

Tato technologie je náhrada čárových kódů. V dnešní době se používá pro označování krabic se zbožím, palet atd. RFID zvyšuje efektivitu sledování zásilek a zboží. Využívají ji také malé obchody, nebo prodejny, ve kterých slouží jako detekce proti krádeži. Technologie má široký rozsah použití podle typu frekvence, které využívá. Levné RFID tagy jsou nejčastěji ve statusu: zapnuto/vypnuto.

Při průchodu z obchodu jsou po stranách antény, které vybudí magnetické pole a při pokusu o průchod s aktivovanou RFID značkou jim bude předána EPC (Electronic Product Code) hodnota, a tím dojde k vyvolání poplachu. Tagy obsahují různé typy paměti pro ukládání informací. „*Paměť pasivních RFID může obsahovat od 1b až po 2kB, RFID tagy jsou schopné zapisovat a číst*“[4].

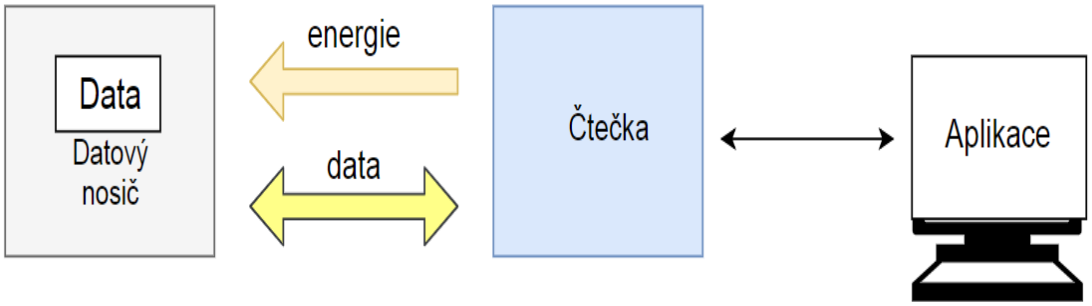


Obr. 1.1: RFID složení.

1.3 Princip komunikace RFID

RFID systém se skládá z těchto části :

1. Koncový systém - zpravidla to bývá databáze (DB). Propojena s aplikací, která může např. otevírat elektronické zámky u dveří.
2. Nosič - objekt, pomocí kterého žádáme o přístup.
3. Čtečka - slouží pro vybuzení signálu / čtení dat.



Obr. 1.2: Princip RFID.

RFID čtečka generuje elektromagnetické pole. V oblasti jeho působení tuto zónu nazveme interakční zónou. Při výskytu RFID prvku v interakční zóně čtečky se vlivem elektromagnetického pole generuje v RFID prvku napětí. Pomocí napětí, které bylo indukováno, se vybudí čip, který je při dostatečné hodnotě napětí schopen vyslat pomocí antény svůj jednoznačný identifikátor, který byl vložen do čipu viz obr.(1.2).

1.3.1 Tagy pro čtení

Tento typ tagů je specifikován vyloženě pro identifikaci předmětů/objektů. V paměti uvnitř tagu můžeme najít unikátní identifikační číslo TID, které bylo vloženo výrobcem. Také ho také můžeme považovat za sériové číslo. Toto číslo není možné žádným způsobem upravovat, více v [4].

1.3.2 Tagy s možností zápisu

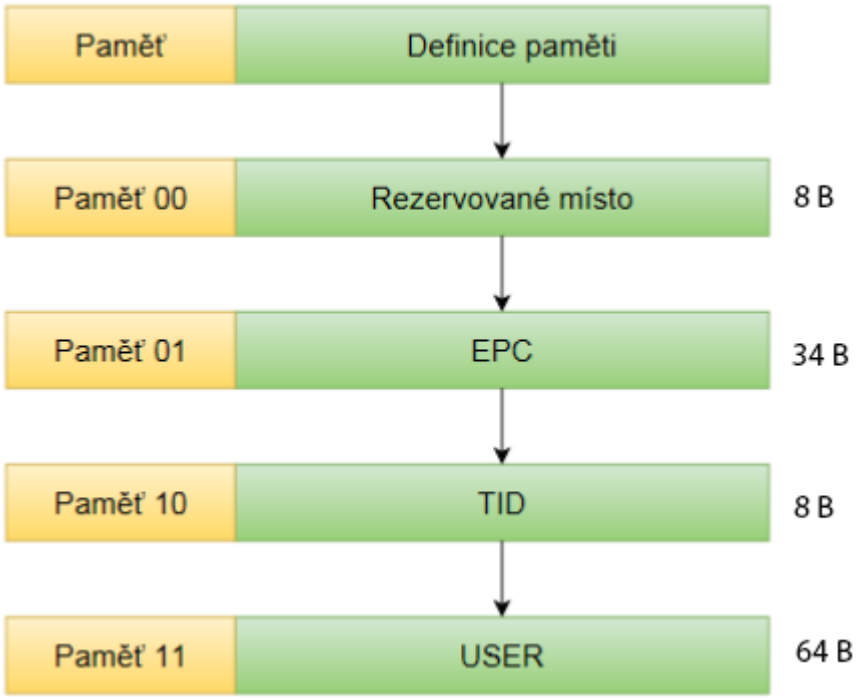
Tagy jsou vyrobeny tak, aby na zařízení vlastník mohl zapisovat data. *"Velmi často je paměť rozdělena na bloky o pevném počtu bajtů. Čtení a zápis dat se pak provádí právě po blocích jakožto nejmenší adresovatelné jednotce paměti"* [6]. Nejprve se musí paměť přečíst, následně dojde k modifikaci jednotlivých bajtů a provede se uložení. Bajty jsou odeslány zpět do tagu, který je již modifikovaný.

U některých tagů je vyžadováno, aby data nemohla být čtena bez autorizace. Jednoduchou obranou proti čtení dat bez povolení je předem získané heslo, které chrání data proti čtení a zápisu. Zde RFID zařízení porovná heslo, které bylo přijaté, s heslem uloženým v paměti. RFID pasivní tagy umožňují následující příkazy pro ochranu nebo zničení tagu.

1. **Heslo pro likvidaci "kill"** – tento příkaz v RFID pasivním tagu slouží pro „zlikvidování“ Elektronického kódu produktu (EPC) hodnoty, která je snímána pomocí čtečky. Hodnota bývá chráněna heslem v paměti RFID prvku. Při zaslání příkazu „kill“ musí dojít k zadání správného hesla o velikosti 32 bitů a EPC hodnota je vymazána. Nejčastěji se provádí v obchodech, v nichž zákazník zaplatí za zboží, jako důkaz, že nebylo ukradeno. Žádný deaktivovaný RFID tag nekomunikuje s čtečkou [12].
2. **Přístupové heslo** – 32 bitové číslo. Tagy, které neobsahují přístupové heslo, musí být neustále ve stavu "lock"pro zapisování dat do paměti.

Demonstrace způsobu uložení dat na u RFID obr. (1.3). Paměť je uložena do bloku o pevné velikosti. Při zápisu dat do paměti je potřeba určit, do jakého bloku paměti zápis provést. Dodatečná data, potřebná zapsat, jsou uložena do Paměť 11. Paměť 11 slouží pro data přidaná uživatelem. Blok USER má předem stanovenou velikost volného zápisu dat.

Tagy zapůjčené z VUT v Brně mají pro jednotlivé části paměti tyto velikosti:



Obr. 1.3: Demonstrace zápisu do paměti.

Nejčastější délka EPC je mezi 96 bitů a 496 bitů. Hodnota TID nejčastěji prezentována délkou 160 bitů. Paměť alokována pro USER může mít různou velikost, která se odvíjí od typu použitého tagu.

1.4 Kolize v RFID a její řešení

Jelikož RFID zařízení komunikují skrze bezdrátové prostředí, vyskytují se šance na kolize. Při výskytu více RFID tagů v oblasti iterační zóny čtečky každý tag reflekjtuje signál vysílaný čtečkou zpátky směrem ke čtečce a dojde k tomu, že je čteno mnoho tagů ve stejnou chvíli. Pro zmenšení šance na výskyt kolizí RFID systém využívá rozdělení komunikačních kanálu pro jednotlivé tagy. Čtečka vyšle každému tagu určitý časový interval, kdy může zasílat data. Typy přístupu k médiu jsou následovné: TDMA (Time Division Multiple Acess), SDMA (Space Division Multiple Access), FDMA (Frequency Division Mltiple Acess) více můžeme najít v [1].

Časový multiplex (TDMA)

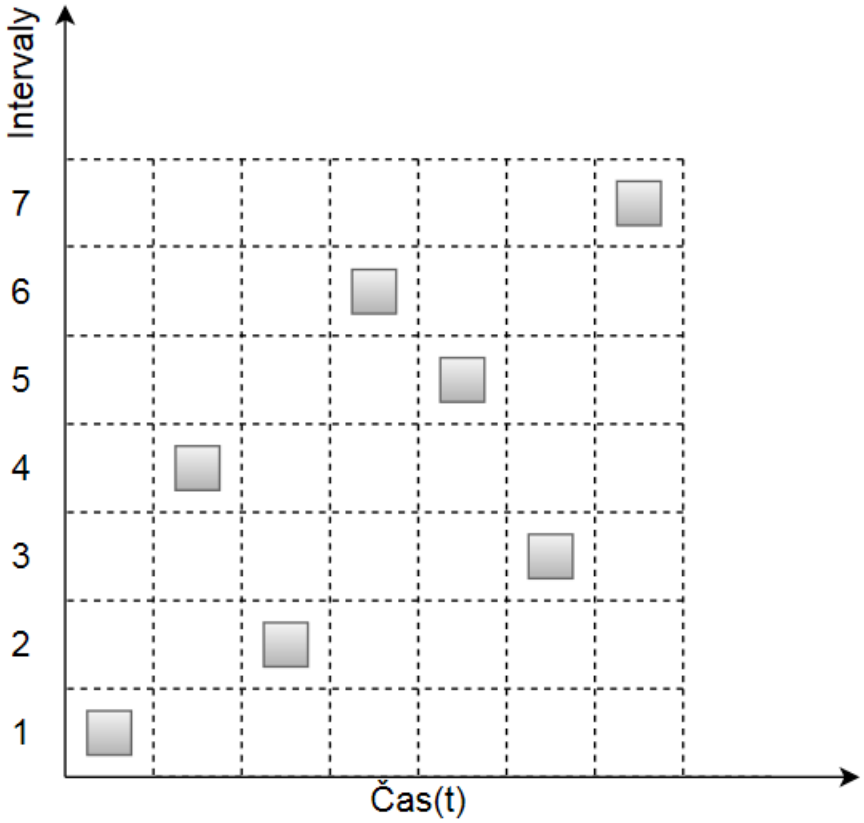
Poskytuje možnost sdílet více zařízením (uživatelům) jeden komunikační kanál, který se děli do více časových úseků. Vysílací kanál je rozdělen mezi jednotlivé tagy. TDMA má největší skupinu anti-kolizních metod. Je přidělen časový úsek pro každou identifikovanou RFID kartu v poli vysílače. Nejlepší způsob, jak se vyhnout kolizi pří výskytu více tagů, je naprogramovat RFID čtečku tak, aby při každém čtecím kole tagy s unikátním ID byly čteny pouze jednou. Máme zde protokoly jako jsou Aloha [15], Stromový protokol [13].

Aloha protokol

Aloha protokol umožňuje náhodný přístup k jednotlivým mediím viz obr (1.4). Jestli se vyskytne zařízení, které potřebuje odeslat data, zašle data bez zjišťování zda je médium volné. Pokuď vysílá jedno zařízení a zároveň zkusí vysílat data druhé zařízení, nastává kolize a tag zkusí kontaktovat čtečku zase za určitou časovou konstantu. S počtem tagů zde také roste délka čekání. Tato metoda je vhodná jen do určitého počtu tagů v oblasti čtečky [15].

Dynamic Framed Slotted Aloha (DFSA)

DFSA je rozšíření protokolů Aloha. Výhodou DFSA je dynamická velikost rámců pro jednotlivá data, která musí být přenášena. V závislosti na velikosti dat protokol mění okno, do kterého tag vkládá data pro svoji identifikaci. Pokud data, která



Obr. 1.4: Princip Slotted Aloha protokolu.

vysílá tag, jsou větší než hranice popisující maximální velikost slotů, jednoduše je další slot přidán. Pokud máme slot, obsahující méně dat než je jeden slot, je hranice minimální velikosti snížena, více v [13].

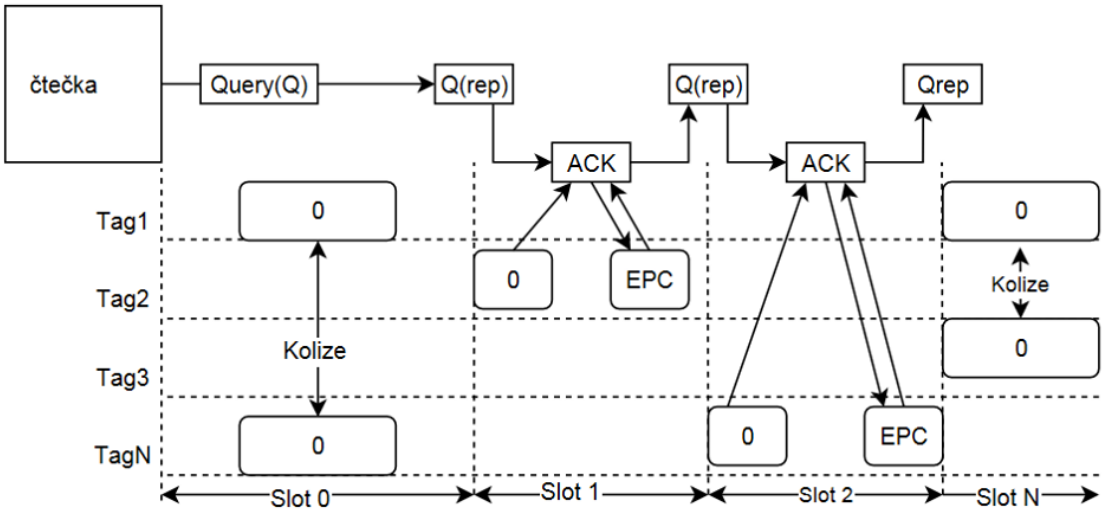
1.5 Standard EPC global class-1 generation-2

GEN2 standart popisuje fyzickou komunikaci mezi čtečkou a tagem. Čtečka zašle informace k tagu modulováním RF (Radio Frequency) signálu. Tag obdrží informaci a energii potřebnou na správnou funkci skrze RF signál. Tag moduluje signál a je vyslán zpět ke čtečce, kde dochází k demodulování signálu a rozpoznání jednotlivých bitů.

Tag odráží data, která jsou kódovaná Millerovým modulováním subnosné (M2, M4,M8). Čísla M jsou typy Millerova modulování, u nichž hodnoty udávají, kolik period popisuje jeden datový symbol. Čtečka a tag mohou komunikovat pouze asynchronně. Buď vysílá data čtečka nebo tag, více v[17].

1.5.1 Anti–kolizní Q protokol pro EPC GEN2

Q protokol je založen na hodnotě Q a funkci 2^Q. Q má rozsah $[0-15]$, pomocí tohoto rozsahu si čtečka vypočítá počet slotů, ve kterých se můžou vyskytovat jednotlivé tagy. Čím vyšší hodnota Q, tím nižší šance kolize. Počet tagů, by měl ležet mezi 30 až 50% rozsahu funkce 2^Q. Tímto můžeme regulovat, že zbylých 50% slotů je nevyužito a schopno obsáhnout další tagy, které by se mohli objevit v průběhu. Maximální hranice počtu na detekci jednotlivých tagů je 32768. GEN2 si můžeme popsat následovně.

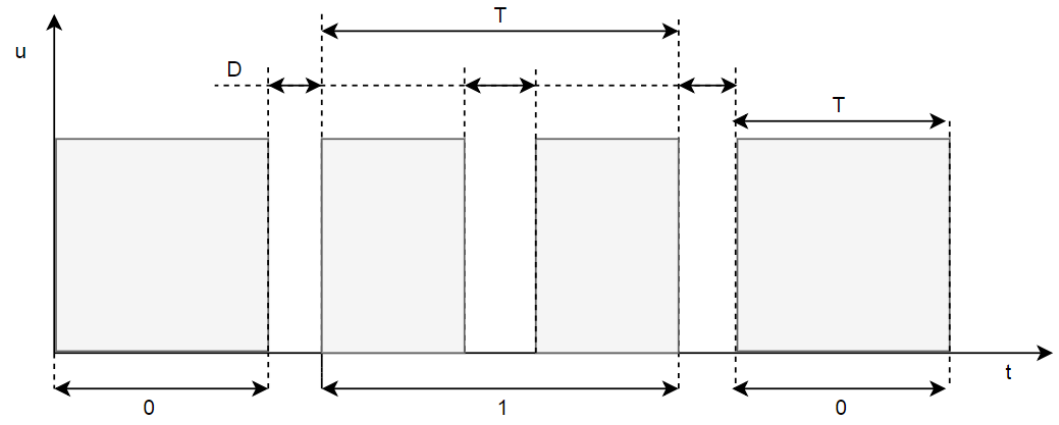


Obr. 1.5: Q protokol.

1. Čtečka pošle rámec přes speciální příkaz s parametrem Q. Každý tag zvolí náhodou hodnotu od 0 do $2^Q - 1$. Tag, který má hodnotu 0, je brán jako první.
2. Čtečka použije příkaz "QueryAdjust", aby každý tag snížil hodnotu o 1. Tag má přiřazen kanál v případě dosáhnutí hodnoty 0.
3. V okamžiku, kdy tag má přiřazen komunikaci, zašle pouze krátký paket obsahující ID. GEN2 standart toto ID vyjadřuje jako "RN16"(náhodné číslo velikost 16 bitů). Obdrží–li čtečka odpověď od jednoho tagu, obdrží tento paket úspěšně a nebyla zjištěna žádná kolize viz obr. (1.5).
4. Čtečka může provádět příkazy jako čtení dat, zapisování dat a změnu hesla až po obdržení ID. Také si lze vybrat individuální tag po zadání ID.
5. Čtečka také může zaslat příkaz "Silence". Umlčené tagy nadále nebudou posílat svoje údaje.
6. Čtečka může použit příkaz "QueryAdjust", dokonce i když nebudou všechny tagy na hodnotě 0. Při zasláni příkazu všechny umlčené tagy vygenerují nové hodnoty podle nové velikosti okna. Více informací najdeme v [18].

1.5.2 Komunikace čtečka–karta

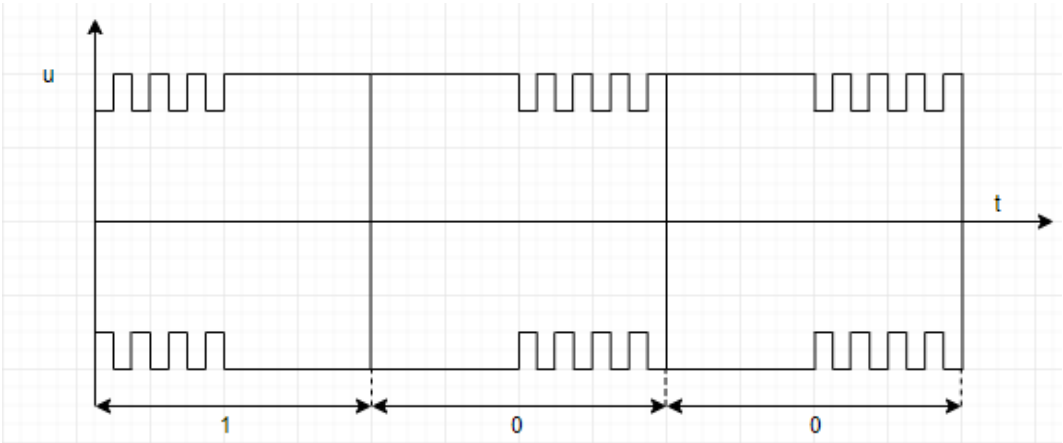
Základ přenosu je dán časem T, který nám určuje, jak dlouho se vysílá jeden bit. Pro kódování bitů je použit Millerův modifikovaný kód, který se přerušuje v čase T na dobu D (doba přerušení) obr. (1.6). D je ve vztahu s časem T tak krátká, aby kondenzátor udržel napětí na kartě a držel kartu v chodu po časovém intervalu T. „*Hodnoty bitů jsou dány pozicí přerušení D v intervalu T*“.



Obr. 1.6: Komunikace čtečka – karta.

První bit hodnoty 0 zde dostaneme po uplynutí časového intervalu T bez přerušení. Bit hodnoty „1“ se v půlce časového intervalu T přeruší na dobu D a pokračuje po zbytek doby T. Poslední bit hodnoty 0 je vysílán opět bez přerušení. Jak můžeme na obr. (1.6) vidět, nadcházející hodnoty se kódují podle předchozí.

1.5.3 Komunikace karta–čtečka



Obr. 1.7: Komunikace karta – čtečka.

Po zátěžové modulaci probíhá následné kódování. "*Jestliže nastanou čtyři pravidelné poklesy amplitudy signálu v první polovině doby trvání bitu T*"[14], značí to situaci, kdy byl vyslán bit hodnoty 1. Jestliže obdržíme sekvenci v druhé polovině intervalu T, znamená to bit hodnoty 0 (obr.1.7). Tato kapitola čerpá ze zdroje [14] společně s kapitolou 1.5.2.

1.6 Bezpečnost RFID

Jelikož RFID je používán k přenosu dat v bezdrátovém prostředí, vyskytuje se zde mnoho možností jak napadnout tento systém. Lze útočit na datový nosič, čtečku a také na přenos signálu.

1. Deaktivování tagu
   Útok je zde představen jako typ útoku, kde čtečka neví, zda se v oblasti vyskytuje RFID tag. Můžeme např. vložit kovový objekt mezi čtečku a tag. Nebo vytvořit silné elektromagnetické rušení. Další způsob je trvalá destrukce tagu (odlomení antény), fyzické poškození.
2. Útoky pro ovlivňování běhu systému (DOS– Denial of services)
3. Zachycení komunikace
   Pokud má útočník dostatečně silnou anténu, která je naladěná na stejnou frekvenci jako RFID systém a zároveň má zvolenou správnou modulaci. Je zde riziko odposlechnutí až na vzdálenosti desítky metrů. Pro úspěšnost útoku je vyžadováno schopnost následně dekódovat data.

1.6.1 Útoky na RF přenos signálu

Útoky nejsou prováděny pouze na zařízení, které nese informace, ale také na část autentizace, kdy se data přenáší z datového nosiče do čtečky přes bezdrátové prostředí. [11]

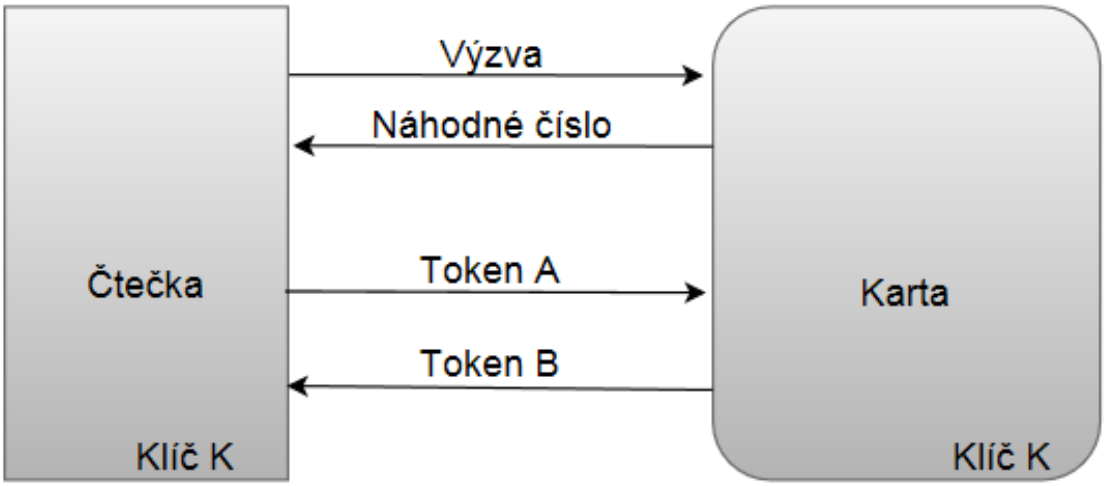
Odmítnutí služby (DOS)

Útoky lze realizovat pomocí rušení frekvence mezi čtečkou a datovým nosičem. Dojde k zahlcení frekvence, na které je uskutečněn přenos dat. Protože RFID je bezdrátová technologie a používá k přenosu dat elektromagnetické pole, které působí na určité frekvenci. Další možnost je útočit přímo na tag a snaha o jeho deaktivaci pomocí příkazu „kill“ [12]. Tagy mají omezenou paměť a tato hesla mohou být jednoduše zlomena pomocí „hrubé síly“. Tagy, které jsou levné, nemají implementované žádné protokoly, které by ověřovaly funkci čtení. Ochrana na DOS útoky může být např: izolovat prostor ve kterém čtečka snímá.

Útok opakování zprávy (replay attack)

Útok spočívá v napadení probíhající komunikace výzva – odpověď. Tento způsob je nejvíce využíván pro RFID autentizace. Útočník zachytil komunikaci mezi čtečkou a tagem, následně zachycenou komunikaci nahraje na svoje zařízení. Díky zachycené komunikaci se může se vydávat za platný RFID tag. Obrana je zde při aplikování kryptografických mechanismů, jako je generování náhodného čísla pro každé ověření. Autentizace nesmí obsahovat totožné informace jako v předešlé autentizaci, více v [16].

1.6.2 Výzva–odpověď



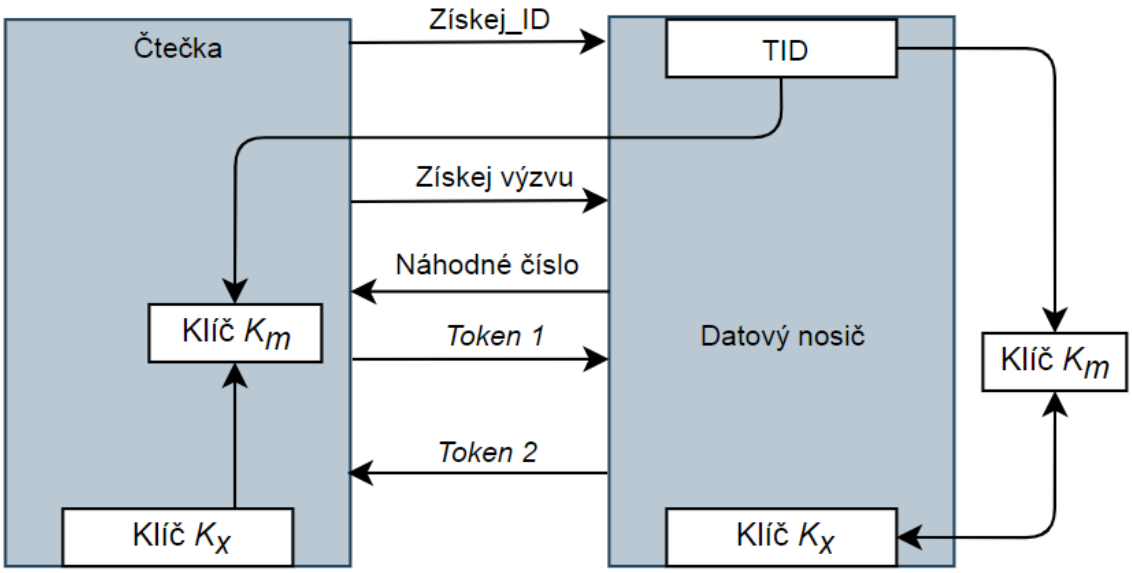
Obr. 1.8: Autentizace pomocí výzva – odpověď.

Datový nosič dostane výzvu, generuje náhodné číslo obr. (1.8). Čtečka generuje náhodné číslo a pomocí známé šifrovací funkce zašifruje její generované číslo a obě čísla zašle kartě. Datový nosič dešifruje (Token A) a jestli najde v dešifrovaném textu svoje původní číslo, tak klíče sedí. Vygeneruje další náhodné číslo sloužící pro ověření, pošle společně s předchozím číslem (Token B), které generovala čtečka. Ověří zda číslo, které poslala v prvním kole, se rovná číslu přijatému teď. Toto je důkaz, že oba klíče sedí ke stejné aplikaci.

Velkou nevýhodou může být, že všechny datové nosiče patřící pro jednu aplikaci, obsahují stejné klíče. Toto je velice nebezpečné. Můžeme najít miliony nosičů pro jednu aplikaci se stejným klíčem pro výměnu dat.

1.6.3 Derivované klíče

Každý datový nosič má unikátní klíč. Při výrobě jednotlivých datových nosičů se zároveň přečte jejich identifikační číslo obr. (1.9). Systém je stále založen na symetrické kryptografii, K_x jsou klíče tajné, pomoci kterých se vypočítá master klíč K_m, který je použit následně pro výměnu. Master klíč je odvozen pomocí klíče K_x a předem definované funkce. Následné autentizace pokračuje podle [1.6.2]. Tato kapitola s kapitolou [1.6.2] byly zpracovány podle [1].



Obr. 1.9: Odvození klíče pro výměnu.

1.7 NFC technologie

Near field communication (NFC) není typ RFID systému. Je to pouze způsob, jak je možné přenášet data mezi dvěma zařízeními. Tento způsob komunikace můžeme přirovnat k *Bluetooth* technologii.

Datový přenos mezi dvěma těmito zařízeními využívá HF na rozsahu 13,56 MHz. Dosah zařízení pro datový přenos je do 20 cm, protože druhé komunikující zařízení je přiloženo do velké blízkosti získáváme název NFC. Pro komunikaci mezi dvěma přístroji musíme rozeznávat 2 typy NFC zařízení.

- **NFC iniciátor** – slouží pro zahájení komunikace.
- **NFC cíl** – je zařízení, s kterým iniciátor komunikuje.

Technologie má největší uplatnění pro placení pomocí mobilních zařízení. Taktéž může být využita pro přenos souboru mezi zařízeními podporující NFC jako jsou telefony s androidem [1]. Nejnovější možnost NFC je autentizace místo RFID zařízení.

Zaměstnanec dostane služební telefon, který může použít zároveň jako autentizační prvek.

- **Pasivní mód** – Bývají v provedení štítků nebo nálepek. Stejně jako u RFID není zde vyžadován dodatečný zdroj energie. U tohoto druhu NFC není možno se propojit s jinými aktivními prvky jako je telefon. Slouží jen pro přečtení.
- **Aktivní zařízení** – Zde patří chytré telefony, čtečky karet a platební terminály. Díky většímu výpočetnímu výkonu a dodatečnému zdroji energie tato zařízení jsou schopna odesílat a přijímat data. Je zde možnost komunikace mezi dvěma aktivními NFC zařízeními.

2 Představení základních principů identifikačních systémů

Elektronické přístupové systémy využívají přenosné datové nosiče na automatizované ověřování autorizace na přístup do objektů. Při ověřování existují 2 typy systémů.

- **Online systémy**
- **Offline systémy**

2.1 Online systémy

Online systémy jsou nejčastěji nasazovány tam, kde je velké množství kontroly příchozích, kteří musí projít autorizací v rozmezí několika sekund. V takové situaci si můžeme představit vstupní bránu do závodu firmy. V systému jsou všechny terminály spojeny s hlavním zařízením, kterým je centrální počítač. Na tomto CPC (centrální PC) je spuštěna DB (databáze) a každý vstupní terminál je pomocí vnitřní sítě propojen společně. Navíc jsou terminály spojeny s CPC, aby mohly kontrolovat řízení přístupu pomocí tabulky z DB. Data z DB jsou uložená v každém přístupovém prvku (čtečka) a tam jsou uchována v podobě tabulky. Využívají síť, která propojuje všechny terminály, aby každý měl přehled o celém záznamu.

Pokud je požadavek na změnu, musí být upraven záznam na CPC, kde se edituje tabulka záznamů. Po úpravě se automaticky aktualizuje a každý terminál má k dispozici tabulku, ve které jsou nově uložené změny. Výhodou je, že celý areál vybavený terminály pro řízení přístupu je chráněn proti neoprávněnému přístupu. Datové nosiče, které jsou využity na online systémy, musí být schopny uchovat pouze malé množství dat.

2.2 Offline systémy

Systémy jsou převážně nasazovány v situacích, kde je mnoho oblastí, do kterých má přístup minimální počet lidí, a zároveň musí vlastnit elektronické zařízení pro přístup. Všechny systémy uchovávají záznamy klíčů a ty popisují, pro které terminály má jaký klíč přístup. Na rozdíl od online systému je zde vše uloženo v terminálu a nenajdeme tu žádný CPC nebo síť, která je propojena s ostatními terminály.

Informace určující, k jakým terminálům má subjekt přístup, je uchována na elektronickém nosiči dat. Na tomto nosiči je informace uložena ve formě tabulky, v níž jsou klíče sloužící pro identifikaci jednotlivých místnosti (Sauna – 584). Při požadavku o přístup je celý seznam z terminálu porovnán s tabulkou datového nosiče,

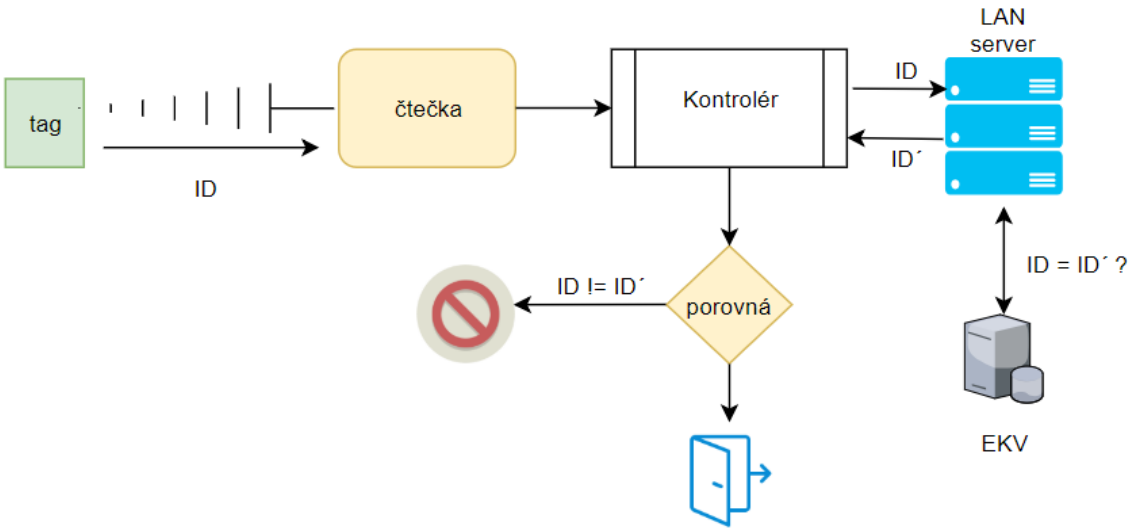
následné povolení přístupu je uděleno po nalezení shody v terminálu a datovém nosiči.

Datový nosič je naprogramován na hlavní „programovací stanici“, kde mohou být nastaveny přístupy pro jednotlivé subjekty. Přístupy mohou být dány pouze na určité dny, následně se deaktivují. Kapitola čerpá ze zdroje [1] spolu s kapitolou [2.1].

2.3 Moderní autentizační a identifikační systém

Autentizační systém

Za moderní systém mohou být považovány takové systémy, které k autentizaci osob využívají pomocný back-end systém sloužící pro porovnávání přijatého ID z karty s DB. DB má uloženou tabulku záznamů, kde specifikuje pravidla pro uživatele. K autentizací pomocí RFID můžeme připojit kontrolér, který se bude starat o funkci elektronických zámků k jednotlivým vstupním terminálům obr. (2.1). Více informací nalezneme v [14].



Obr. 2.1: RFID systém v kombinaci s EKV.

Identifikační RFID systém

Za identifikační považujeme takový systém, který detekuje přítomnost předmětu. Osoba se tomuto systému nemusí nijak prokazovat, protože od systému nežádá žádnou akci k provedení. Jako identifikační systém můžeme uvažovat senzory rozmístěné po trasách pro běžce na dlouhé vzdálenosti. Lze kontrolovat, zda proběhli jednotlivými stanovišti úspěšně a nebo také jejich průměrnou rychlost.

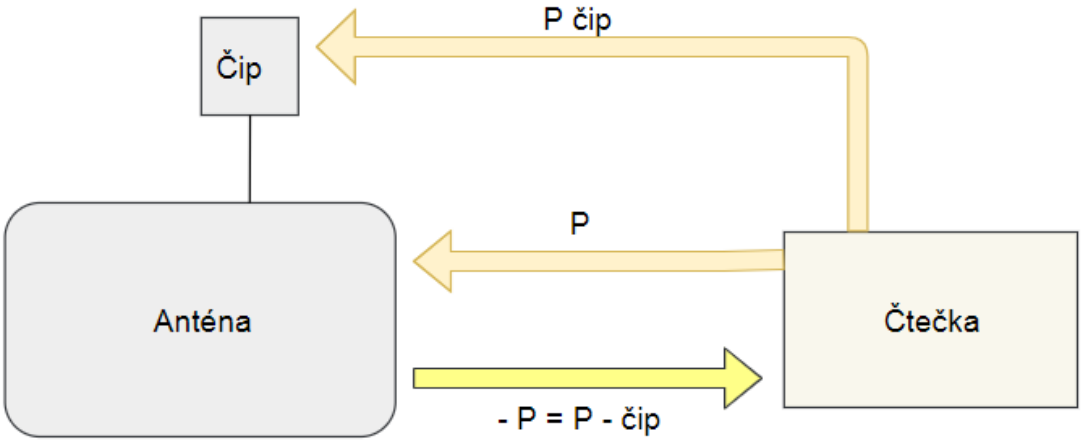
3 Aktivní a pasivní RFID zařízení

Důležitou vlastností prvků je, jak se potřebná energie pro správnou funkci dodává a jak je energie využívána. RFID prvky s mikroprocesorem zpracovávají operace náročné na energii jako jsou kryptografické výpočty. Zde můžeme rozlišit RFID prvky na aktivní a pasivní.

3.1 Pasivní RFID

Pasivní prvky nemají dodatečný zdroj energie, ale s využitím antény datový nosič získá dostatečné množství energie, která vystačí na pokrytí spotřeby RFID datového nosiče obr. (3.1). Energii získá při okolním působení magnetického nebo elektromagnetického pole, které vzniká v oblasti čtečky. Je zde aplikován mód RTF (Reader Talk First).

Na přenos dat mezi datovým nosičem směrem ke čtečce, můžeme využít modulaci pole, které vytváří čtečka. Datový nosič muže dočasně uchovat energii, aby mohla probíhat komunikace ve směru čtečka → datový nosič a zároveň i obráceně datový nosič → čtečka. Pokud je ovšem pasivní RFID prvek umístěn mimo pole čtečky, nemůže dojít k výměně informací mezi těmito dvěma prvky.



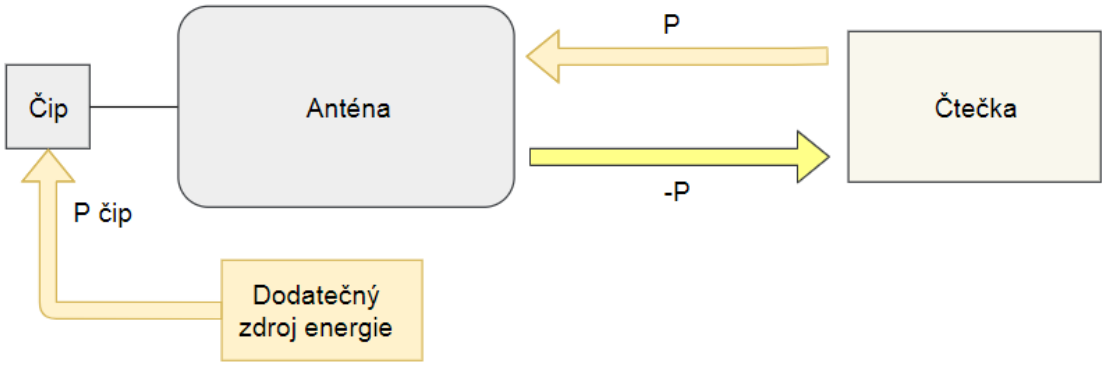
Obr. 3.1: Schéma pasivního prvku.

3.2 Aktivní RFID

Aktivní RFID prvek má dodatečný zdroj energie. Nejčastěji je využita dodatečná baterie nebo solární prvek obr. (3.2). Účel dodatečného zdroje energie je pro vybuzení dostatečného napětí pro čip. Magnetické nebo elektromagnetické pole zde není

vyžadováno pro napájení čipu. Elektromagnetické nebo magnetické pole, které vybudí čtečka, zde může býti mnohem slabší než u systémů, ve kterých se využívají pasivní RFID prvky [1]. Pole slouží jen pro přenos dat.

Pokud máme datový nosič s dodatečným napájením, je schopný detekovat slabší signál, který vydává čtečka. Toto může zvýšit dosah komunikace mezi čtečkou a datovým nosičem. Ovšem ani aktivní RFID prvek není schopný generovat vlastní signál, tyto prvky dokáží modulovat signál čtečky, aby proběhl přenos dat mezi datovým nosičem a čtečkou. Vlastní zdroj energie zde neslouží tedy k tomu, aby dokázal přenášet data bez pole, pouze k tomu, že se slabší signál moduluje a následně proběhne přenos dat mezi RFID prvkem a čtečkou [19]. Aktivní prvky vybavené dodatečným zdrojem energie dosahují větších vzdáleností pro úspěšné identifikace.



Obr. 3.2: Schéma aktivního prvku.

Hodnota P zde prezentuje energii dodanou čtečkou. Zde vidíme výhodu aktivních RFID, protože podle síly signálu zde zvětšujeme vzdálenost použití. Tag pro funkci čipu využívá svůj zdroj energie.

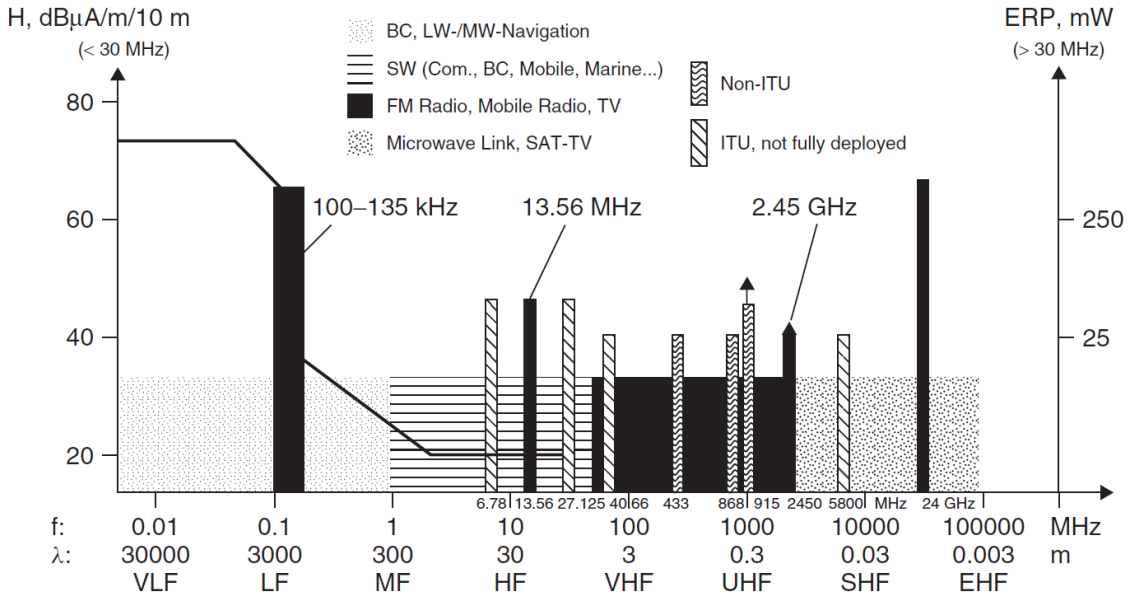
3.2.1 Porovnání aktivního a pasivního RFID

Tab. 3.1: Porovnání aktivních a pasivních RFID.

Vlastnosti	Aktivní RFID	Pasivní RFID
Paměť	Podle typu tagů	Desítky Bitů
Dosah(m)	Až stovky metrů	Desítky m v závislosti na čtečce
Cena	Až 100x dražší než pasivní	Nejlevnější v řádech Kč
Zabezpečení	Kryptografické moduly	Nejčastěji hesla pro paměť
Napájení pro čip	Dodatečná baterie	Indukované z přijatého signálu
Přenos	Asynchronní	Asynchronní

3.3 Frekvence a rozsahy

RFID systémy produkují a vyzařují elektromagnetické vlny. Tyto systémy mohou být nazývány také jako rádiové systémy. Nesmí narušovat služby ostatních rádiových systémů například rádiových služeb, televizního vysílaní a bezpečnostních složek. Nesmí také zasahovat do pásma (průmyslového, vědeckého a lékařského).



Obr. 3.3: Frekvenční rozsahy [převzáno z [1].

Důležitý parametr v RFID systémech je volba správného pásma a tedy i frekvence, kterou budeme využívat. Nejčastěji se používá 135 kHz pro RFID s krátkým dosahem. Je to vhodná frekvence využívající silného magnetického pole pro induktivně spojované systémy (pasivní RFID). Dále zde máme frekvence, na kterých se provozují už RFID systémy s vyšším dosahem, které obsahují širokou škálu rozsahu od 135 kHz do 5,8 GHz viz obr. (3.3). Mikrovlné systémy využívají rozsah 2.45 až 5.8 GHz používají elektromagnetické pole. Operační frekvence je taková frekvence, kterou čtečka vysílá. Frekvence, kterou vysílá datový nosič, se nebere v potaz, nejčastěji však jejich frekvence jsou totožné, více informací najdeme v [1].

3.3.1 Nízké frekvence 100-150 KHz

RFID systémy s malou vzdálenosti se nejčastěji používají v systémech, kde je vyžadována velká bezpečnost. Není zde ale vyžadována velká vzdálenost, jelikož se v těchto případech musí RFID zařízení přikládat na předem určené místo nebo do vzdálenosti centimetrů od určeného zařízení. Používají indukční spojování, aby získali energii na

komunikaci se čtečkou. Je zde nejmenší přenosová rychlost v porovnání s ostatními frekvencemi pro RFID. Obvykle obsahují malé množství dat potřebné pro přenos, neobsahuji anti–kolizní protokoly.

3.3.2 Vysoké frekvence 3-30 MHz

Známé pod názvem vzdálené přístupové systémy. Mají dosah do 1 metru. Velká výhoda systému může být v jeho rychlosti, která je vyšší než u LF, ale nižší než u UHF. Typ RFID prvků se střední frekvencí může být vybaven anti–kolizním systémem. Tudíž nedochází k problémům při čtení prvků, pokud máme v okolí čtecí zóny více prvků. Zpravidla se tu ale anti–kolizní protokoly neaplikují, protože dosah čtečky není tak velký, aby bylo nutno protokoly aplikovat. Frekvence využívána pro tyto tagy je 13,56 MHz a jejich velikost v případě čipových karet je kolem 10 cm.

3.3.3 Velmi vysoké frekvence 868 MHz 2,4 GHz

Systém, který dokáže zapisovat a číst do vzdálenosti 10 metrů u pasivních RFID. Má velkou rychlost čtení. Nejčastěji můžeme najít v systémech, v nichž je potřeba identifikovat na velké vzdálenosti i ve velké rychlosti. Je zde vyžadováno, aby identifikátory měly vlastní zdroj energie, takže se používají s kombinací s aktivními prvky. Aplikují se u systému jako je vybírání mýtného pro automobily.

Nevýhoda této frekvence nastává, když systém umístíme do vlhkých oblastí. Frekvence není schopna dobře proniknout skrz kapaliny a nedokáže číst identifikátory, které můžeme také maskovat pomocí lidského tepla. Kapitoly 3.3.1, 3.3.2, 3.3.3 popisující úrovně frekvencí jsou čerpány z [5].

3.3.4 Srovnání frekvencí u RFID technologie

Tab. 3.2: Tabulka pro RFID frekvence.

Frekvence	Dosah	Uplatnění	Nevýhody
100-150 Khz	V řádech cm	přístupové systémy	malá rychlost čtení
13,56 Mhz	do 1m	nasazení v průmyslu	kov snižuje dosah
868 Mhz	do 10m(Evropa)	elektronické mýtné	Kapaliny pohlcují signál
2,4 Ghz	Aktivní stovky m	vybíraní mýtného	náročné konstrukce

3.4 Představení současných principů metod a schémat pro autentizaci a identifikaci entit

Kapitola sepsána podle standartu 9798-5 [20]. Standart popisuje autentizaci entit a mechanismy využívající techniku nulových znalostí.

3.4.1 Mechanismy založené na identitách

Entity, které žádají o přístup, musí být rozdělené do skupin. Ke každé skupině náleží právě jedna akreditační autorita. Akreditační autorita je důvěryhodná strana, které věří všichni členové skupiny. Nárokující strana musí vlastnit identifikační data, řetězec bitů, s kterými dále pracujeme. Délka je omezena podle standartu. Při použití Hašovací funkce musí být domluvena specifická funkce známa pro všechny identity. Akreditační autorita zde generuje soukromé informace pro autorizace.

1. Strana A (nárokující strana) zvolí náhodné číslo r, které je uchováno v tajnosti. A vypočítá svědka pomocí $W = r^v mod(n)$. Kde W je svědek, r je náhodné číslo a v je veřejný akreditační ověřovací exponent, n vyjadřuje součin prvočísel p a q.
2. A pošle $Token_1$ straně B (dokazovací strana) kde $Token_1$ musí byt roven hodnotě W.
3. B získá $Token_1$ a zvolí náhodnou posloupnost celých čísel od $d_1, d_2 \dots d_m$, kde posloupnost čísel představuje výzvu.
4. B odešle výzvu $d_1, d_2 \dots d_m$ straně A.
5. A vypočítá odpověď D z hodnoty r a soukromé informace akreditace.
6. A posílá $Token_2$ ke straně B.
7. pokud ověřovací výpočet sedí, a W=W‘, potom je proces platný. Jinak strana B zamítne stranu A.

3.4.2 Mechanismy založené na asymetrickém šifrování

Jestli mají entity využívat asymetrické šifrování, je potřeba ustanovit společnou h(f) a typ asymetrického systému. Musí také vlastnit dvojici klíčů S_k a V_k. Délka těchto klíčů je závislá na typu použité asymetrické šifry.

1. Strana B zvolí náhodné číslo r a je uchováno v tajnosti. B vypočítá $r||h(r)$. $Token_1$ který obsahuje výzvu (d) je poslán nárokující straně A zašifrován ve tvaru $d = V_k(r||h(r))$.
2. Strana A použije soukromou transformaci pro získáni hodnoty $r||h(r) = S_a(d)$.
3. A pošle $Token_2$ entitě B kde musí platit r=D, tak B příjme A.

3.4.3 Technika nulových znalostí

Riziko klasických asymetrických systémů se zde snaží být minimalizováno. Při odpovědi pro ověřovací stranu v asymetrických systémech používáme soukromý klíč pro potvrzení výzvy. Zde může nastat potencionální nebezpečí zjištění klíče. Jestli nárokující strana zvolí výzvu vhodně, je schopná dopočítat S_k žadatele.

Princip nulových znalostí je zde použit pro vhodnou konstrukci zpráv. Nárokující strana nemůže zjistit soukromý klíč strany, která žádá přístup.

Strana B je schopná určit pouze, zda tvrzení od strany A je pravdivé nebo nepravdivé. Celá komunikace probíhající se stranou A by mohla být také simulována pouze stranou B. Nedozví se zde tedy žádné tajné informace strany A.

4 Měření pomocí RFID systému Roger

V kapitole je popsáno měření RFID čtečky Roger AS 3992x a antény UHF915M-ANTPCR. V dokumentaci od výrobce je uvedeno, že tento systém patří mezi systémy dosahující středního dosahu (1-5 m) při použití zmíněné antény s 8 dBm zesílením. Maximální výstup toho systému dosahuje 20 dBm síly výstupu.

Využívá Deanse Reader Mode (DRM). DRM mód znamená, v případě zjištění další čtečky na stejné frekvenci se komunikace převede na jinou frekvenci např z 868 MHz ⇒ 869 MHz. Nedochází tedy k rušení signálů. Pro měření a simulace byl použit software AS399x Reader Suite. Rychlost čtení by měla být do 6 ms. RFID systém se skládá z následujících prvků.

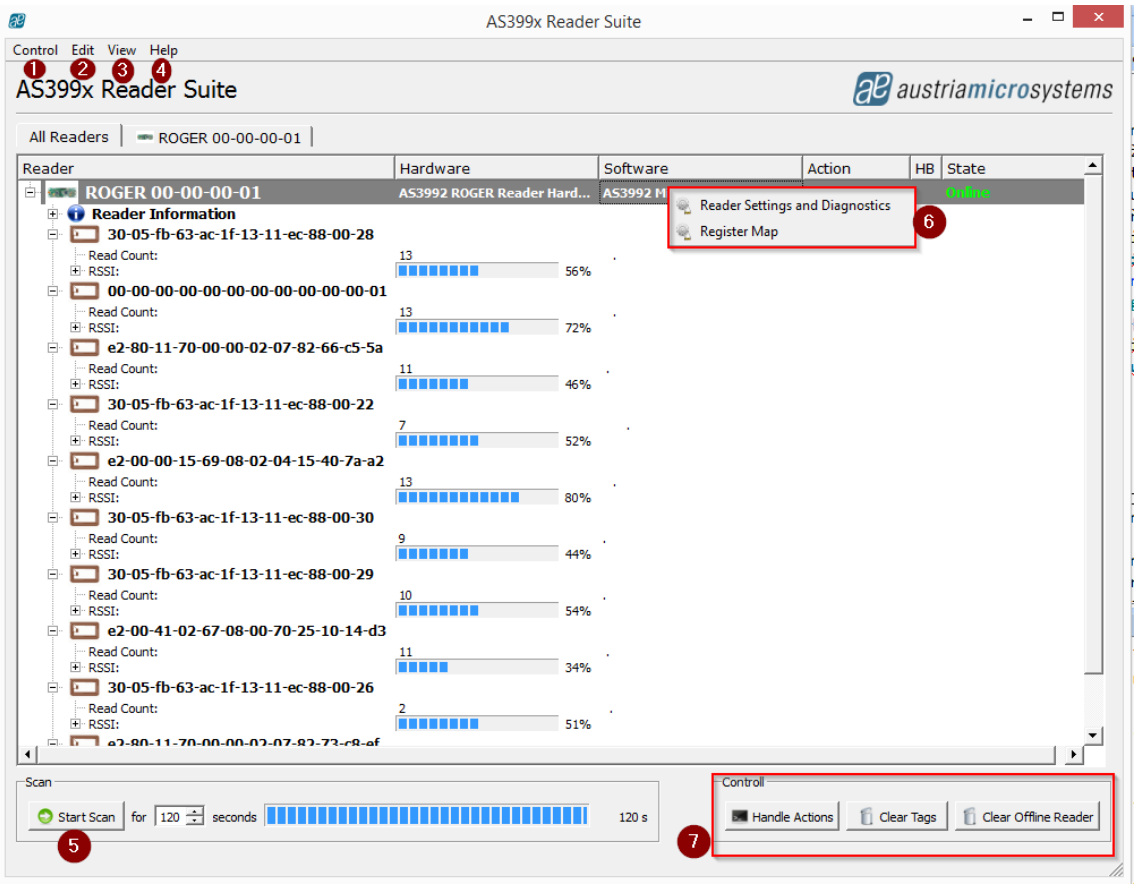
1. Roger 3992x reader
2. UHF915M-ANTPCR anténa
3. USB kabel mini
4. PC, na kterém běží program Reader Suite.
5. Adaptér pro napájení +3,3 3,6V/2A

4.1 Využití čtečky

Roger čtečka je pouze pro zapisování a čtení tagů, po obdržení příkazu kontrolerem.

4.1.1 Popis programu Reader Suite

1. Control menu – Slouží pro začátek skenování tagů, nebo lze použít tlačítko číslo 5 (obr.4.1).
2. Otevře dialog – Ve kterém lze konfigurovat následné: Časový úsek, pro který budou tagy zobrazeny v hlavním okně. Automatické smazání po čase, kdy se tváří tag jako neaktivní. Vymazání záznamu o tagu po uplynutí předem určeného času, kdy je mimo pole. Uživatel zde může nastavit jméno pro tag místo hodnoty EPC. Aktivování/deaktivování sledování komunikace mezi čtečkou a tagem. Nastavování trvání slotů pro více čteček viz (obr.4.1).
3. View menu – Slouží pro dodatečné informace o čtečce a tagu.
4. Help – Pro zobrazení GUI verze a kontaktních informací dodavatele.
5. Start Scan – Slouží pro spuštění skenování, vedle se nachází časový interval na který aktivujeme čtečku a můžeme skenovat tagy.
6. Pravým klikem na čtečku dostanem nabídku, ve které lze konfigurovat nastavení čtečky.
7. Control panel – Obsahuje základní funkce jako jsou: Vyčištění záznamu tagů, smazání neaktivních čtecích zařízení a tlačítko Handle actions, které musí být



Obr. 4.1: popis programu Reader Suite.

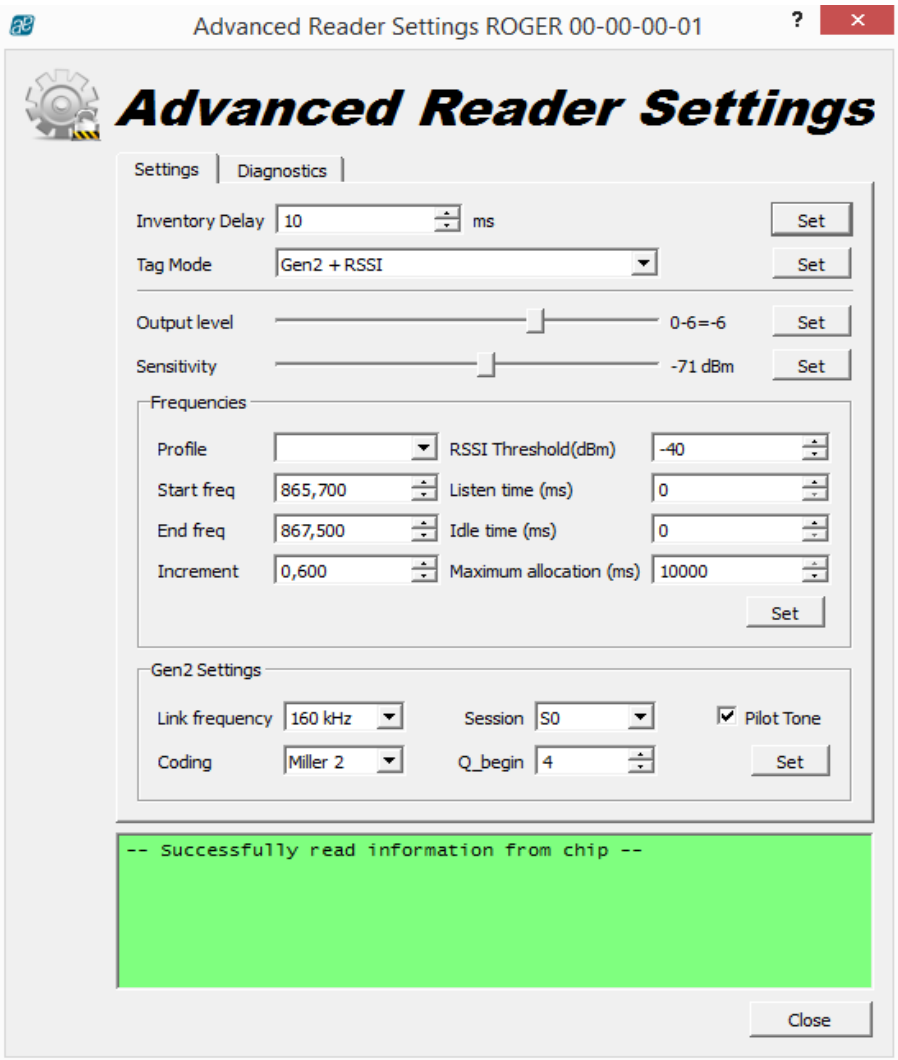
aktivní, pokuď je nastavena akce pro tag, která má být spuštěna po jeho detekování.

Na hlavní obrazovce jako první záznam je uvedena čtečka, která je momentálně připojena.

Nastavení pro čtečku se provede pomocí Advanced Setting pravým klikneme na RFID čtečku. Následně se nám otevře okno jako je na obr. (4.2).

- Tag mode – přepínaní mezi Gen2, Gen2+RSSI, ISO 6B.
- Output level – nastavuje výstupní hodnotu signálu pro RFID systém. Maximum je označeno hodnotou "0".
- Sensitivita – popisuje schopnost čtečky reagovat na různé síly signálu směrem od tagu.
- Profile – přednastavené profily pro Evropu, Ameriku, Čínu, které jsou popisovány standarty.
- RSSI Threshold – popisuje jakou silou se vrací signál odražený od tagu.
- Gen2 – parametry pro nastavení GEN2.

V záložce diagnostic jsou nástroje pro detailnější zkoumání síly signálu při určitých frekvencích. V sekci sweep lze spustit různé typy kmitočtu na měření.



Obr. 4.2: Nastavení parametru pro čtečku.

- Reflected power radar – ukazuje sílu odraženého signálu na určené frekvenci.
- Continuous Modulation – v tomto módu je neustále vysílán příkaz NAK.

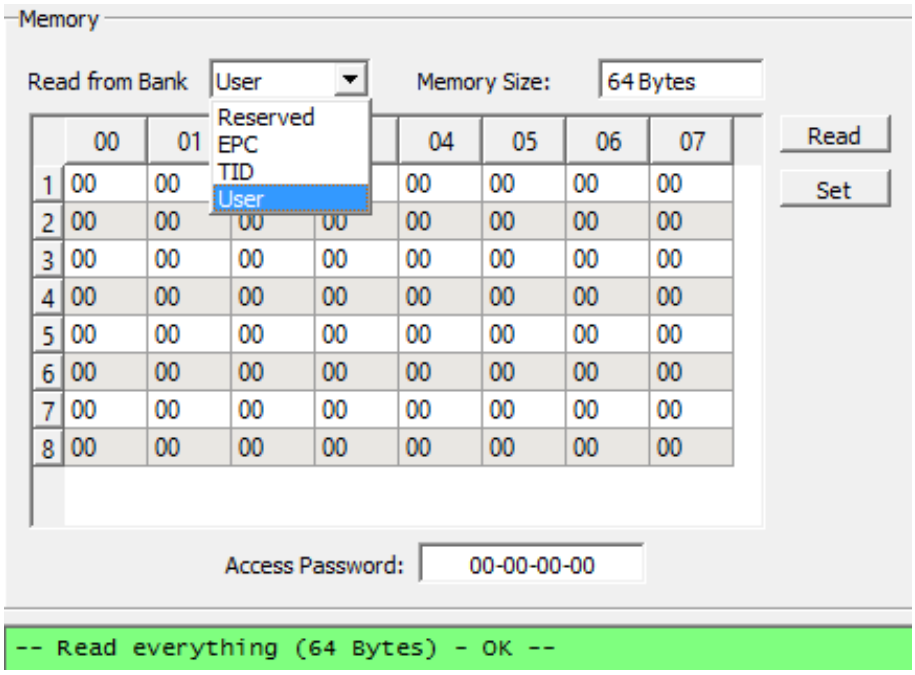
Register map obr. (4.2) otevře menu, kde je možnost konfigurovat RFID čtečku, pokuď není potřeba nechat na základní nastavení. Vždy je načteno výchozí nastavení po připojení čtečky k napájení. Pro konfiguraci na delší vzdálenosti bylo nutno měnit i toto nastavení.

4.1.2 Možnost nastavování RFID tagu

Pravým kliknutím na načtený tag přes funkci Advanced Tag Settings lze přenastavovat informace pro tagy.

Nastavení a příkazy pro tagy

- Nastavení EPC – uživatel je schopný přenastavit EPC výchozí, na svoje zvolené EPC.
- Nastavení hesla – může být nastaveno heslo pro přístup a vymazání tagu.
- Zamknutí tagu – uživatel je schopný provést zamykání a odemykání jednotlivé části paměti.
  1. Kill – Slouží pro deaktivaci tagu.
  2. Acess – Při nastavení této hodnoty je potřeba zadat heslo pro přístup.
  3. EPC – Elektronické identifikační čislo, lze nastavit heslo na jeho čtení.
  4. TID – Identifikační číslo dané při výrobě.
  5. USER – Paměťový prostor, do kterého může zapisovat uživatel libovolná data.



Obr. 4.3: Čtení dat z paměti.

Uživatel může měnit jednotlivé části paměťového prostoru (EPC,USER) kromě místa, které je rezervované trvale v paměti a TID dané při výrobě.

Tagy lze také přejmenovávat, aby se nám nezobrazovalo EPC, ale alias. Tag si lze pojmenovat podle libovolného uvážení, zároveň je možné přiřadit obrázek. Ke každému tagu lze přiřadit aplikaci, která se má spustit, pokuď je tag identifikován.

5 Měření parametrů

V kapitole jsou shrnuty jednotlive výsledky měření, které byly prováděny na RFID systému pro pasivní UHF tagy. Výsledky jsou prezentovány formou tabulek a grafů. V tabulkách můžeme vidět výrobcem udávané vzdálenosti pro jednotlivé tagy a skutečné vzdálenosti, které byly změřeny pomocí zapůjčeného systému Roger.

5.1 Měření vzdálenosti jednotlivých tagů

Dosah tagů je uváděn do vzdálenosti 10 m. Při využití roger čtečky, která má dosah 1-5 m byly naměřeny tyto maximální vzdálenosti viz tab. (5.1). Sloupec EPC obsahuje pouze poslední 2 čísla z 96 bitového řetězce.

Tab. 5.1: Měřené vzdálenosti karet.

EPC	Síla signálu(dBm)	Naměřená vzdálenost(m)	Schopnost čtečky.
22	20	4,2	<5 m
26	20	4,2	<5 m
28	20	4,5	<5 m
29	20	3,7	<5 m
30	20	4,7	<5 m

Další měření probýhalo pro tagy typu "IQ". Proti RFID kartám viz tab. (5.1), které jsou specifikovány pouze na nekovové materiály. IQ tagy jsou speciálně navrženy na různé typy povrchů viz tab. (5.2), jako jsou železné a plastové podložky.

Tab. 5.2: Speciální IQ tagy.

	Dosah(m)	Použití	Změřená vzdálenost(m)
IQ150	1,6	všechny materiály	1,6
IQ400P	5	plasty	2
IQ400	4,2	plasty+nekovy	1
IQ600	6	všechny materiály	3,1
IQ800P	10	Plasty	5

Podle různých typu tagů zde také můžeme vidět různé velikosti v paměti tab (5.3).

Dodatečné testy pro měření

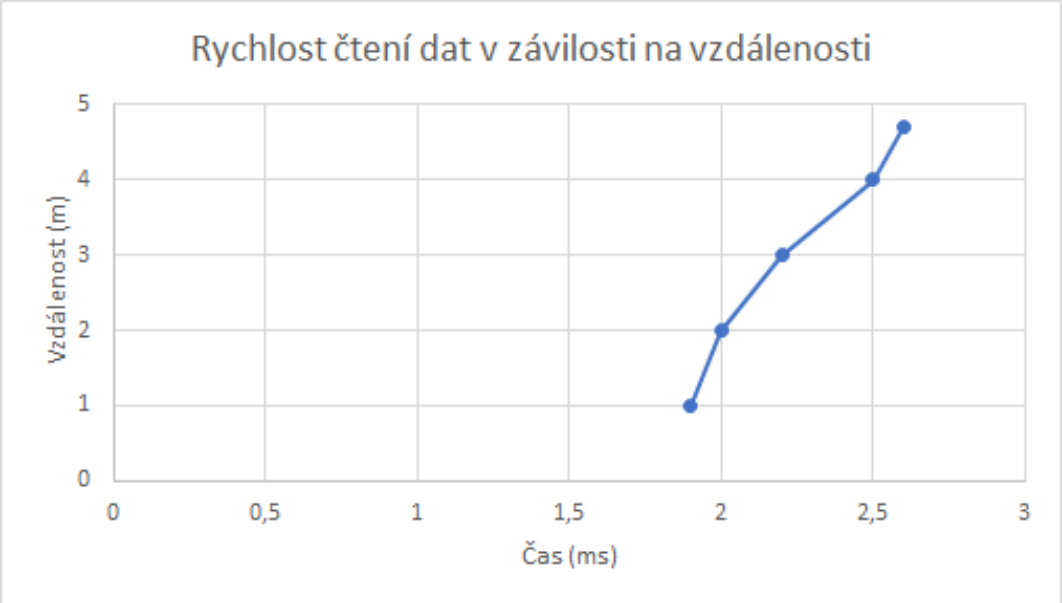
Při vložení kovového objektu mezi tag a anténu nebylo schopné tento tag identifikovat, stejná situace nastala i při vložení kapaliny před UHF kartu.

Při vyzkoušení změření semi–active tagu, který dosahoval až vzdálenosti 6,3 m. Bylo dokázáno, že při vyšší síle signálu bychom byly schopni změřit i pasivní UHF tagy na delší vzdálenost.

Tab. 5.3: Rozdíly v paměti pro IQ tagy.

	EPC(bits)	USER(bits)	TID(bits)
IQ150	96	64	48
IQ400P	96	512	64
IQ400	96	64	48
IQ600	96	64	48
IQ800P	96	512	64

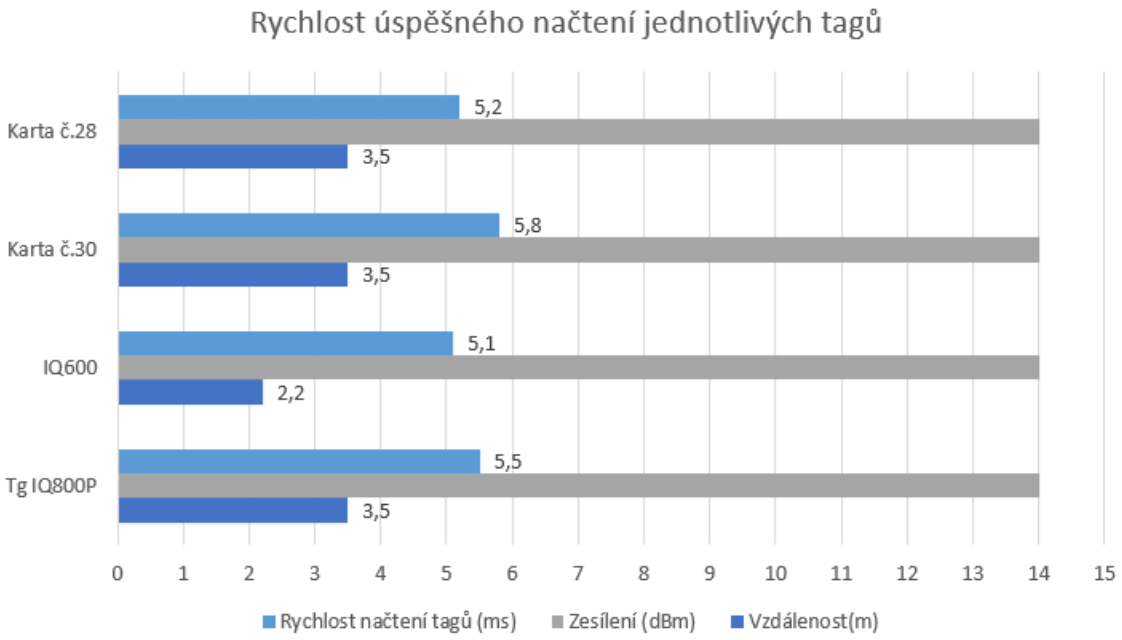
5.2 Rychlosti načtení tagů v závislosti na vzdálenosti



Obr. 5.1: Měření vzdálenosti načtení tagu v závilosti na čase.

Měření (5.1) demonstruje pouze, za jakou dobu RFID čtečka ví o tagu, který je vložen do její integrační zóny. Tag lze není zcela přečten, ale je pouze detekován. Je to konec kroku, který čtečka nazývá "inventory". Zde dochází k detekování tagů pro další postup obr. (5.3).

Jak je demonstrováno na grafu obr. (5.2), zde je je časový interval pro úspěšné přečtení kompletního tagu minimálně jednou takový. Je zde měřen i jiný typ tagů. *IQ* tagy je možné použit pro kovové a plastové materiály.



Obr. 5.2: Vyjádření vzdálenosti a úspěšné přečtení tagů.

Graf viz obr. (5.2) popisuje kompletně načtený tag bez přenosových chyb.

5.3 Měření chybovosti v závislosti na vzdálenosti

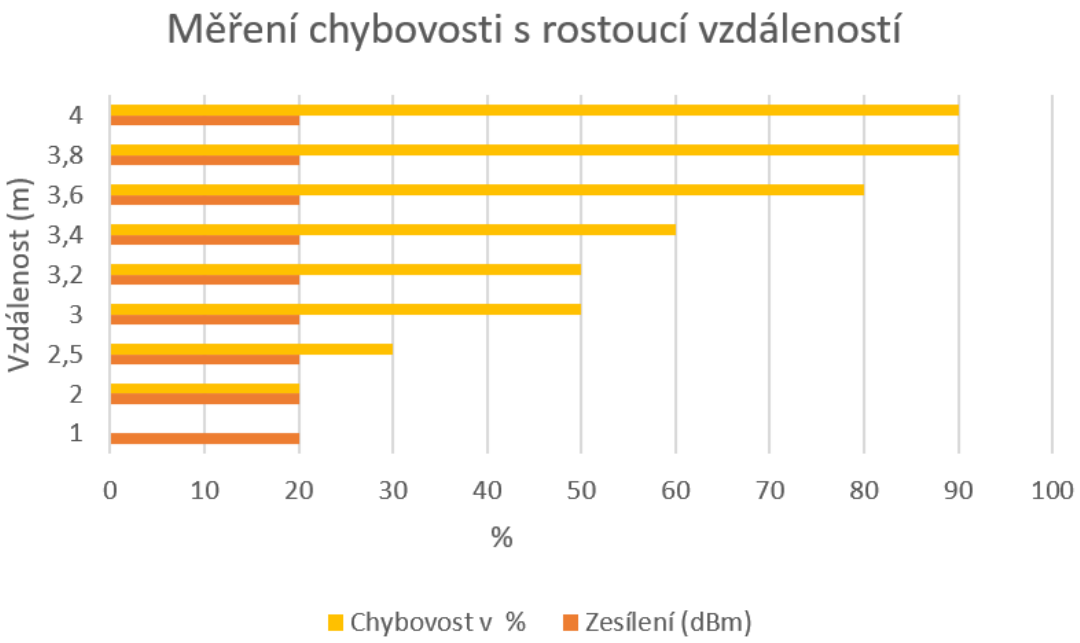
Jednotlivé operace čtečky pro výběr tagu

1. **Select** – pro rozhodnutí, která skupina tagu bude odpovídat.
2. **Inventory** – rozeznání jednotlivých tagů ze skupin.
3. **Access** – tag již byl potvrzen, paket ACK spolu s "RN16"byly potvrzeny a nyní lze provádět operace s tagem.

```
- -Inventory found 1 EPCs
- --Found EPC: 30-05-fb-63-ac-1f-13-11-ec-88-00-29       freq=866900 kHz, RSSI ea
- Found 3 tags: 30-05-fb-63-ac-1f-13-11-ec-88-00-26 30-05-fb-63-ac-1f-13-11-ec-88-00-22 30-05-fb-63-ac-1f-13-11-ec-88-00-29
- Got from the reader: >>ROGER 00-00-00-02<< the EPC: 30-05-fb-63-ac-1f-13-11-ec-88-00-26
- -> handleNewTags
- No configuration for tag...
- Got from the reader: >>ROGER 00-00-00-02<< the EPC: 30-05-fb-63-ac-1f-13-11-ec-88-00-22
- -> handleNewTags
- No configuration for tag...
- Got from the reader: >>ROGER 00-00-00-02<< the EPC: 30-05-fb-63-ac-1f-13-11-ec-88-00-29
- -> handleNewTags
- No configuration for tag...
- Trying to do an inventory
```

Obr. 5.3: Detekce počtu tagů.

Program Reader Suite neukazuje při zapnutí sledování přenosu dat chybovost. Kde je pro měření chybovosti využit Cyclic Redundance Code (CRC-16), je to způsob, jak detekovat chyby při přenosu. Na obr. (5.3) o lze vidět, že jsou detekovány 3 tagy a tag s číslem 26 má svojí hodnotu 0, tag ihned vyšle "RN16"(16-bitové náhodné číslo), které ve výpisu nelze vidět.



Obr. 5.4: Měření chybovosti.

Pomocí programu Reader Suite a jeho GUI byl otevřen log pro sledování příkazů, které provádí čtečka. Následně byl zvolen výchozí inventory round, od kterého bylo napočítáno dalších 10 iterací. V těchto kolech bylo vidět, kolikrát čtečka extrahovala ID z tagu a byla vypočtena chybovost obr. (5.4).

6 Implementace autentizačního protokolu na platformu BasicCard

Cílem implementace bylo realizovat zabezpečenou autentizaci na procesorové karty označované jako BasicCard. Protokol stojí na ustanovení šifrovacího klíče pro AES s 256 bit klíčem. Klíč pro šifrování je ustanoven pomocí Diffie-Helman protokolu na eliptických křivkách. Výhoda využití eliptických křivek je zde, že délka parametrů může být mnohonásobně menší než u šifer jako je RSA.

Při využití eliptických křivek se vyměňuje pouze veřejný klíč. Soukromý klíč generovaný každou stranou zůstává utajen a není ho možné dopočítat při vhodně zvolených parametrech. Problém je postaven na diskrétním logaritmu $g^x \ mod \ p$.

Při realizaci protokolu vznikly 2 implementace, které byly nasazené na reálnou kartu. První implementace obr. (6.2), kde karta počítá pouze hodnoty $K_{R1-ID-G1}$ a hodnotu R_1 karta prezentuje stranu klienta. Druhá realizace je pro stranu ověřovatele,který využívá SAM modul (čipová karta). U této realizace jsou prohozené výpočty pro kartu a terminál. Hodnoty vypočítané kartou obr. (6.2) jsou nyní počítané terminálem. Terminál počítá hodnoty určené pro kartu.

6.1 Představení karty a komunikace s terminálem

Pro implementaci protokolu byla využita BasicCard Professional 7.6 rev D. V protokolu se využívá AES šifrování a kryptografické funkce jako je SHA-256. Proto karta, na kterou má být zaveden protokol, musí obsahovat co-processor, který je určen pro výpočty.

Karta kromě RAM paměti a procesoru také obsahuje EEPROM (Electrically Eresable, Programmable Read-Only Memory) paměť, která slouží jako "hard disk"karty. Paměť typu EEPROM obsahuje kód uživatele, který byl napsán v Basicu a také konečná data, jež jsou zapsaná do této paměti, zůstanou uchována, i když karta ztratí napájení.

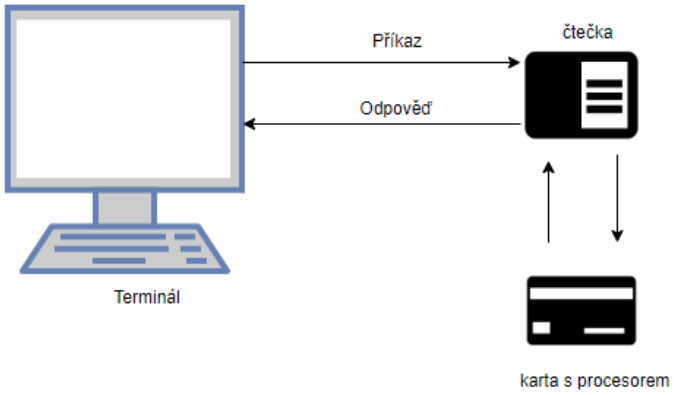
Komunikace u karet obsahující processor je realizována pomocí příkaz-odpověď komunikace. Při vložení karty do čtečky je možné ovládat komunikaci pomocí příkazů.

Procesorová karta obr. (6.1) je pouze pasivní účastník komunikace. Terminál pošle jako první resetující příkaz a následně karta neprovádí žádné operace, dokud neobdrží příkaz od terminálu. Po zaslání odpovědi na daný příkaz karta čeká na další příkaz ze strany terminálu.

Aplication Protocol Data Unit– APDU

Application protocol data unit (APDU) je protokol pro komunikaci mezi čtečkou a chytrou kartou. Pro komunikaci můžeme rozlišovat APDU příkazy a APDU odpovědi. Příkaz je poslán čtečkou a obsahuje 4 Bajtovou hlavičku povinou a 2 nepovinné údaje jako jsou Lc, Le. Hlavička obsahuje CLA, INS, P1, P2. APDU odpověď je vyslána kartou k čtečce a obsahuje povině 2 statusové bajty (SW1, SW2). Jednotlivé údaje znamenají:

- **CLA** – Instruction class – Indikuje typ příkazu.
- **INS** – Instruction code – Indikuje určitý příkaz (zapiš data).
- **P1-P2** – Instrukční parametry pro příkaz (do kterého souboru zapsat data).
- **Lc,Le** – Lc parametr označuje počet bytů v datovém poli. Může být nastaven na hodnotu 0 jestli příkaz nepotřebuje žádné data. Le parametr vyjadřuje jak dlouhý datový výstup může být vygenerován, popřípadě může být i vypnut (disable Le).
- **odpověď SW1-SW2** – Pro úspěšné vyřízení příkazu. Terminál musí přes čtečku obdržet hodnotu 90 00. Tato hodnota vyjadřuje úspěšné provedení příkazu.

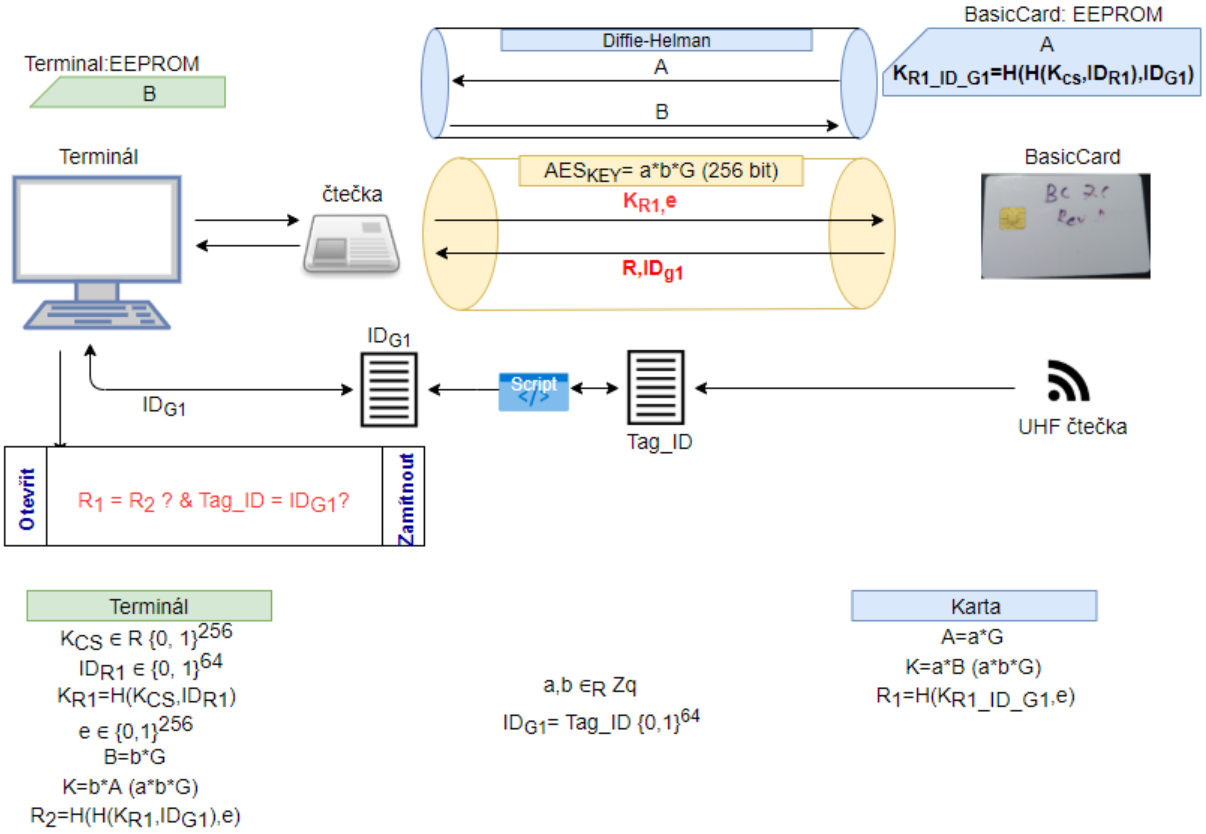


Obr. 6.1: Komunikace terminál-karta.

Parametry Karty (BasicCard Professional 7.6 rev D)

- **EEPROM** – 72 kB
- **RAM** – 4.3 kB
- **Hash** – SHA-224, SHA-256, SHA-384, SHA-512, SHA-1
- **Algoritmy** – DES – Data Encryption standart s délkou klíče 56/112/168 bitu.
  – AES – Advanced Encryption Standard 128/192/256 bitu.
  – EAX – Encryption with Authentication for Transfer (Využíva AES) s délkou klíče 128/192/256 bitu.

6.2 Úprava protokolu



Obr. 6.2: Upravený protokol, terminál je ověřovatel a karta klient.

Protokol byl navržen na VUT v Brně. Protokol je využit pro komunikaci mezi kartami a následné vyhodnocení terminálem, zda autentizace proběhla úspěšně. Při programování protokolu v BasicCard Enviroment ovšem bylo zjištěno, že jestli je potřeba pracovat více jak s jednou kartou zároveň, je zde potřeba využít jiný programovací jazyk, např Java. Prostředí BasicCard Enviroment ale nepodporuje programovací jazyk, který by toto umožňoval.

Schéma realizující stranu uživatele na kartě

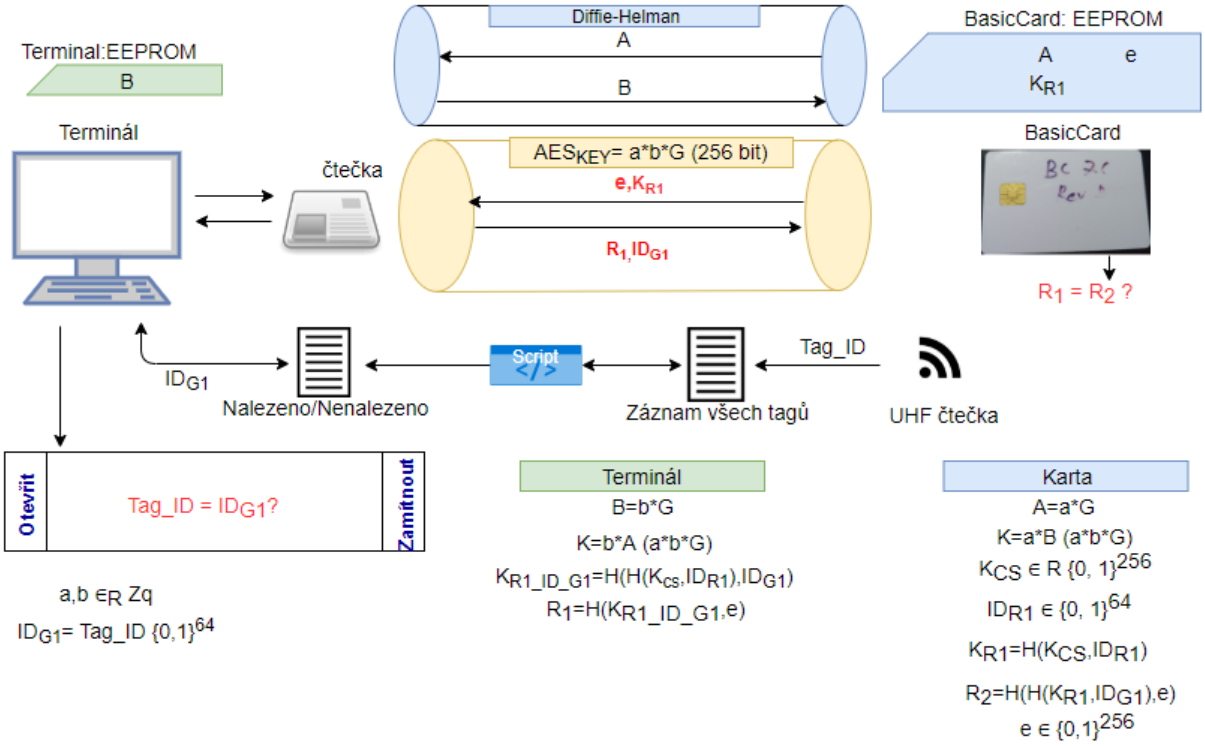
SAM modul původního protokolu je zde simulován jako terminálový program a z toho důvodu není uloženo tolik hodnot do EEPROM paměti. Rozdíl mezi zadaným protokolem a realizovaným je v tom, že není předsdílen veřejný klíč, ale pokaždé se generuje nový soukromý a veřejný klíč pro ustanovení AES klíče a následnou výměnu dat pro úspěšnou autentizaci. Protokol měl obsahovat čtení z online databáze, ale Basic nemá možnost takového čtení. Tato část protokolu byla vynechána. Na kartě byl místo parametru ID_{G1} definován 64 bitů dlouhá hodnota, která je přiřazena jako

jednoznačný identifikátor na kartu a není uložena do EEPROM paměti. Hodnota, která udává jaký identifikátor má mít uživatel u sebe je poslána spolu se zprávou R, která vznikla jako výsledek SHA-256. Byla zde vyřazena část protokolu, kde terminál z přijaté zprávy převezme hodnotu ID_{G1} a následně se až dozví, jaké identifikační prvky by měly patřit do dané skupiny pro kartu.

Jestli by bylo nezbytné mít protokol propojený s databází, bylo by nutné číst data z určitého txt souboru nebo excelu. Z takových souborů je již možné číst, zpracovávat data. Nevýhoda tohoto řešení by mohla nastat po aktualizaci databáze a při každé změně nutno znovu extrahovat aktualizované informace. Bylo by nutné mít vždy aktuální verzi souboru, ze kterého se čtení provádí.

Při úspěšné autentizaci uvidíme výpis v konzoli terminálu, kde bude vypsáno "Autentizace proběhla úspešně". Úspěšné autentizování je doprovázeno zvukem z terminálu. Zvuk by mohl byt nastaven na elektronické zámky a znamenal by povolení přístupu do určité oblasti.

Schéma realizující stranu ověřovatele na kartě



Obr. 6.3: Upravený protokol, kde karta slouží jako ověřující strana, a terminál je klient

Na obr. (6.3) můžeme vidět již zmíněné obrácené výpočty pro kartu a terminál. Terminál zde vypočítá výslednou R_1, která je následně s identifikátorem ID_{G1} za-

slána kartě pomocí AES 256 bit. Karta zde dělá většinu výpočtů a po vypočtení potřebných hodnot jako jsou K_{R1}, R_2 je zkontrolováno zda Hashované hodnoty R_1 a R_2 jsou totožné. Pokuď by byly rozdílné, je na kartě implementovaná podmínka a terminál by neobdržel SW1SW2= 90 00. Bylo by to vyhodnoceno jako „Hodnoty R1 a R2 nejsou totožné“.

Obě schémata jak (6.3) a (6.2) využívají k získání parametru ID_{G1} C sharp script.

6.2.1 Parametry protokolu

Na Basic kartu typu 7.6 rev D jsme schopni nahrát všechny eliptické křivky, které splňují tyto podmínky.

1. Bitová délka parametru $GF_{(p)}$ je mezi 160 a 544 bity.
2. Řád eliptické křivky E je číslo q stejné bitové délky jako p.

Nejdůležitější volbou je, jak zvolit soukromý klíč. Klíč, který je v eliptických křivkách, jež jsou aplikovány v BasicCard Enviroment určen pomocí $1 < S_k < q$. Veřejný klíč patřící k soukromému klíčí následně vypočítáme jako $V_k = [S_k] * G$, kde G je veřejný bod eliptických křivek o délce 256 bitů.

AES klíč je zde při každé autentizaci rozdílný, protože je zde generovaný soukromý klíč $S_k = a, b$ o délce 256 bitů. Po výměně veřejných klíčů provede každá strana násobení bodů eliptických křivek a klíč vychází ze vztahu:

$$\begin{aligned} A &= a * G, \\ B &= b * G, \\ K &= a * b * G \end{aligned} \tag{6.1}$$

Po každém spuštění programu tedy dostaneme rozdílné AES klíče, viz rovnice (6.1). Při vynásobení S_k a V_k dostaneme 512 bitů dlouhý řetězec, z kterého je následně prvních 256 bitů použito jako klíč pro šifrování. Je zde možnost i brát řetězec jiný než prvních 256 bitu pro vytvoření AES klíče, to už záleží na uživateli, kterou část dat o délce 512 bitu si zvolí ve zdrojovém kódu.

6.2.2 Základní metody pro implementaci

Tato sekce stručně popisuje, jaké metody byly použité. Terminálový program se skládá ze 2 částí. Term.zct, který slouží pouze pro vygenerování S_K a V_K karty. Druhá část terminálového programu Protokol test.bas slouží k testování aplikace.

- Card.bas – Zdrojový kód pro kartu.
- Card.def – Vytvořené funkce pro komunikaci mezi kartou a terminálem.
  Ostatní soubory, které jsou zahrnuté, jsou využity jako knihovny pro využívání již existujících funkcí jako je h_f SHA-256.

Terminál jako ověřovatel

- Command H88 H01 GenerujKlice()

  Pro vygenerování S_k a V_k. Karta obdrží příkaz, kde tyto údaje jsou vyjádřené jako 88 01 00 00. CLA= 88, INS= 01, P1= 00, P2= 00.
- Command H88 H03 DostanVerejnyKlic (PublicKey)

  Pro získání veřejného klíče karty.
- Command H88 H06 VytVorKlicProSifru(PublicKey)

  Vypočítá AES klíč pomocí V_k karty a S_k terminálu na straně ověřovatele. Karta zde vypočítá AES klíč jako V_k terminálu a S_k karty. Následně vypočítá AES klíč.

Šifrované přenosy využívající AES 256 bit šifru

- Declare Key 1(16)

  Důležité definovat jak na straně karty, tak i terminálu. Vyjadřuje, že se bude používat AES klíč.
- ProEncryption (P2=1,Rnd,Rnd)

  Zavolání funkce pro šifrování AES 256 bit. P2 zde volí klíč a podle nastaveného klíče je zvolen AES, není zde již potřeba definovat P1="Algoritmus". Rnd hodnoty slouží pro ověření klíče, po ukončení šifrování. Po příkazu Call EndEncryption() a obdržení původních hodnot je prokázáno, že AES klíč je totožný na obou stranách.
- Command H88 H08 Vypocitej $KR1_{IDG1}$ (HashTerminalu,disable Le)

  Předání hodnoty K_{R1} kartě, vypočítání hodnoty R_1 a kní přičtena výzva.
- Command H88 H10 PredejR (R)

  Předání hodnoty R a identifikátoru ID_{G1}

Karta jako ověřovatel

V realizované implementaci jsou metody: GenerujKlice, DostanVerejnyKlic (Lc=0), VytVorKlicProSifru totožné jako v kapitole „Terminál jako ověřovatel". S jediným rozdílem, že obsahují parametry Lc, Le pro rychlejší průběh protokolu.

Hlavní rozdíl je zde v tom, že není jiná možnost, jak udělat protokol, aniž by se nenavazovala 2x šifrovaná komunikace na jeden AES klíč. Bylo zde nutné poslat z karty údaje, pomocí kterých následně vypočítáme hodnotu v terminálu, která se pošle kartě přes šifrovanou komunikaci pomocí AES 256 bit. Při situaci generování nových klíčů pro druhou bezpečnou komunikaci by časová náročnost protokolu vzrostla minimálně o $0,4\,\mathrm{s}$. Rozdílné metody volané na kartě:

- Command H88 H11 Vypocitej$_{KR1}$ (Lc=0,Le=64)

Inicializování výpočtu K_{R1} na kartě. Výstupní data funkce jsou o délce 512 bitů (64 B).

Šifrované přenosy využívající AES 256 bit

Způsob šifrování a nastavení hodnot je zde totožný jako v realizaci programu terminál jako ověřovatel. Rozdíl je zde takový, že šifrování bylo inicializováno 2x. Jednou pro předání hodnot $K_{R1} + e$ ve směru $karta \Rightarrow terminál$. Druhá zabezpečená komunikace využita využita pro zaslání dat $terminál \Rightarrow karta$ pro hodnoty $R_1 + ID_{G1}$.

- Command H88 H13 Predej$_{KR}$ (K$_{R1,E}$,Le=64)

  Slouží k předání hodnoty z karty do terminálu. Parametr K_R a je k tomu přičtená výzva e.
- Command H88 H12 Vypocitej$_{R2}$ (Lc=40,DataZterminalu,disable Le)

  Terminál pošle kartě hodnotu R_1 spolu s identifikátorem ID_{G1}. V této metodě se následně porovná a vyhodnotí zda R_1=R_2.

6.2.3 Měření časové náročnosti

Bylo provedeno měření protokolu jak v kombinaci $terminál \Rightarrow karta$, tak i situace, kdy bylo vše simulováno v terminálu. Při použití karty a čtečky přímo v terminálu nabízí program BasicEnviroment virtuální čtečku a simuluje i kartu.

Tab. (6.1) představuje prezentaci výsledků, jak rychle je protokol schopný běžet v simulovaném prostředí, kde terminál a karta jsou simulovány v PC.

Tab. 6.1: Tabulka měřených hodnot, protokol odměřen virtuálně v PC.

	Terminál-ověřovatel(ms)	Karta-ověřovatel(ms)
AES šifrování	9	22
Výpočet AES pro kartu	32	36
Výpočet AES pro terminál	2	2
Generování klíče karty	35	36
Generování klíče pro terminál	2	2
Časová náročnost programu	598	569

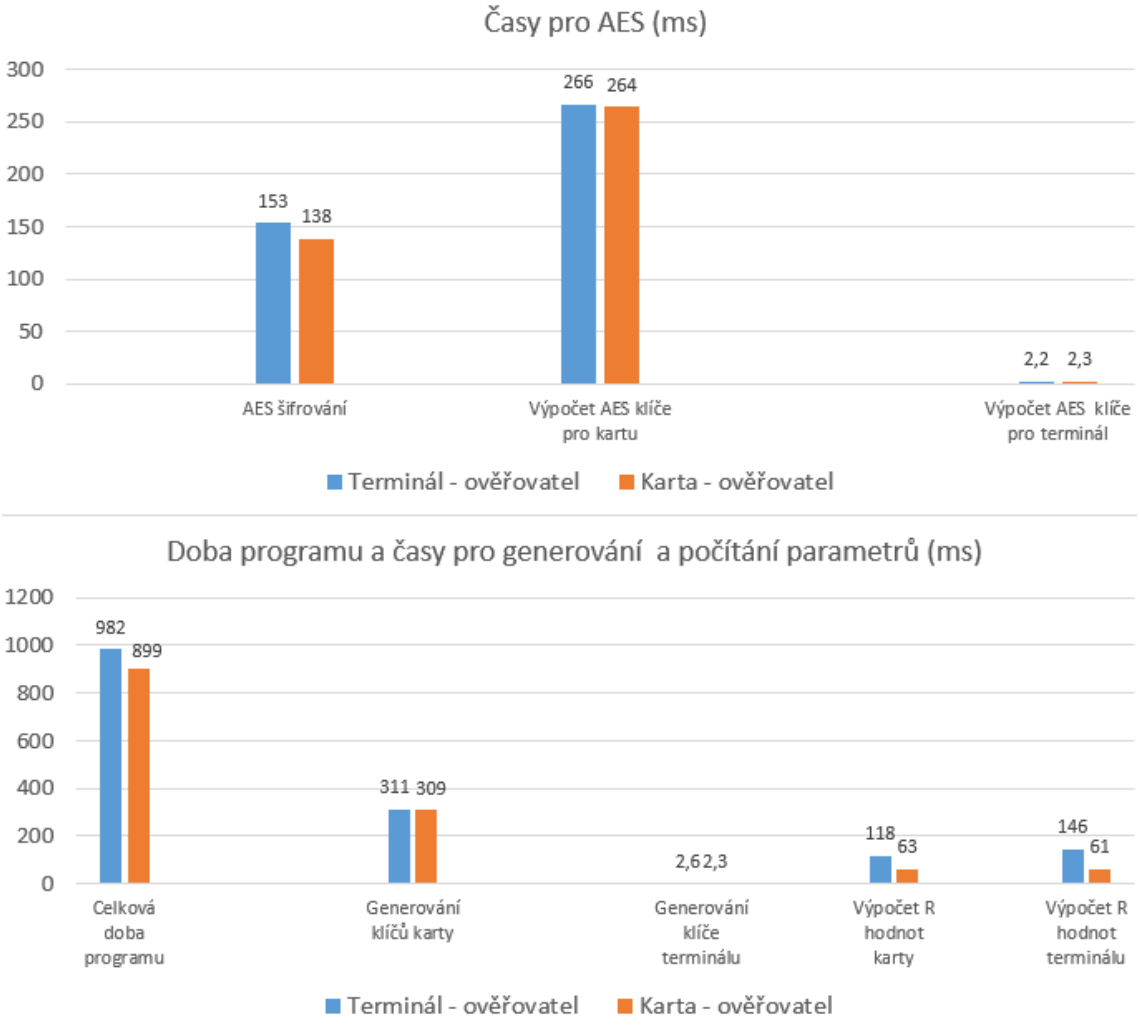
Pro reálné nasazení protokolu na kartu a terminál bylo provedeno měření, při kterém byl program na kartě 10x vyzkoušen a hodnoty zaznamenány. Z tohoto měření byl vypočítán aritmetický průměr měření a výsledné hodnoty jsou prezentovány na obr.(6.4).

Při porovnání výsledků z tab. (6.1) a hodnot z obr. (6.4) můžeme říct, že program ve virtuálním prostředí, které poskytuje Basic Enviroment pro vývoj Basic karet, je

zhruba o 1/2 rychlejší než reálná aplikace. Čas se týká celkové doby programu. Jednotlivé funkce jako např: generování klíčů pro kartu je v průměru o 276 ms rychlejší než u aplikace nasazené na reálný hardware.

Protokol aplikovaný na kartu

Největší rozdíl je zde v situaci, kdy se porovnávají celkové doby programů. U realizace „karta jako ověřovatel“, byly nastaveny Lc a Le parametry. Dalo se tedy porovnat, o kolik bude zhruba rychlejší karta se správně nastavenými parametry Le a Lc oproti terminálu. Program „terminál jako ověřovatel“ tyto parametry nemá nastavené u každého příkazu, jednotlivé operace trvají déle. Je potřeba zjistit, jak velká data budou přijata a odeslána. Nebo zda funkce má vůbec nějaké vstupní a výstupní parametry.

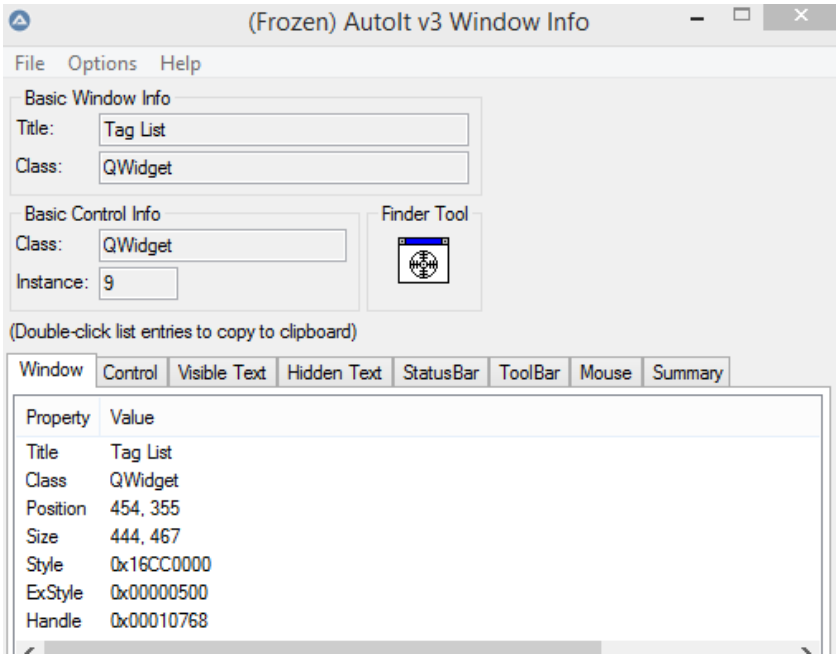


Obr. 6.4: Přehled měřených časů pro jednotlivé operace.

6.2.4 Získaní ID tagu z UHF čtečky

V originálním zadání protokolu je UHF čtečka, která předává přímo naskenované informace do terminálu. Bohužel pomocí programu Reader Suite k zapůjčené čtečce tento program neumožňuje ukládat jednotlivé záznamy. Jednotlivé funkce poskytované programem ke čtečce byly prohledány a nebyla nalezena funkce, pomocí níž by šlo exportovat záznam tagů z existujícího GUI do txt souboru.

Po neúspěšném prohledání funkcí programu byl proveden pokus překompilovat program v programovacím jazyce C. Tento pokus byl ovšem také neúspěšný, jelikož program je natolik komplikovaný, že po načtení zdrojového kódu a snaze ho spustit, nastalo hned několik chyb v prostředí Visual Studio, které hlásilo chyby při kompilaci. Při odstranění jedné chyby se zde vyskytlo několik dalších, které navazovaly na úpravu původní. Tento pokus o vytvoření funkce, která by byla implementovaná do GUI a umožňovala uložit záznam o tagách a následné zpracování, byl neúspěšný.



Obr. 6.5: Získaní parametru okna.

Poslední krok, který byl vyzkoušen, byl proveden v programovacím jazyce C sharp. Princip byl postaven na programu jménem AutoIt Window info obr. (6.5). Tento program je schopný identifikovat jednotlivé vlastnosti jako jsou jméno okna, ve kterém se text vyskytuje a pozici, kde je okno otevřeno na monitoru obr. (6.5).

Po přečtení vlastností pro okno (objekt), v němž se vyskytoval záznam o tagách, byla snaha tento text zkopírovat do textového souboru, ve kterém by se nacházel všechen záznam tagů, které byly naskenovány za určitou časovou dobu. ID tagu by

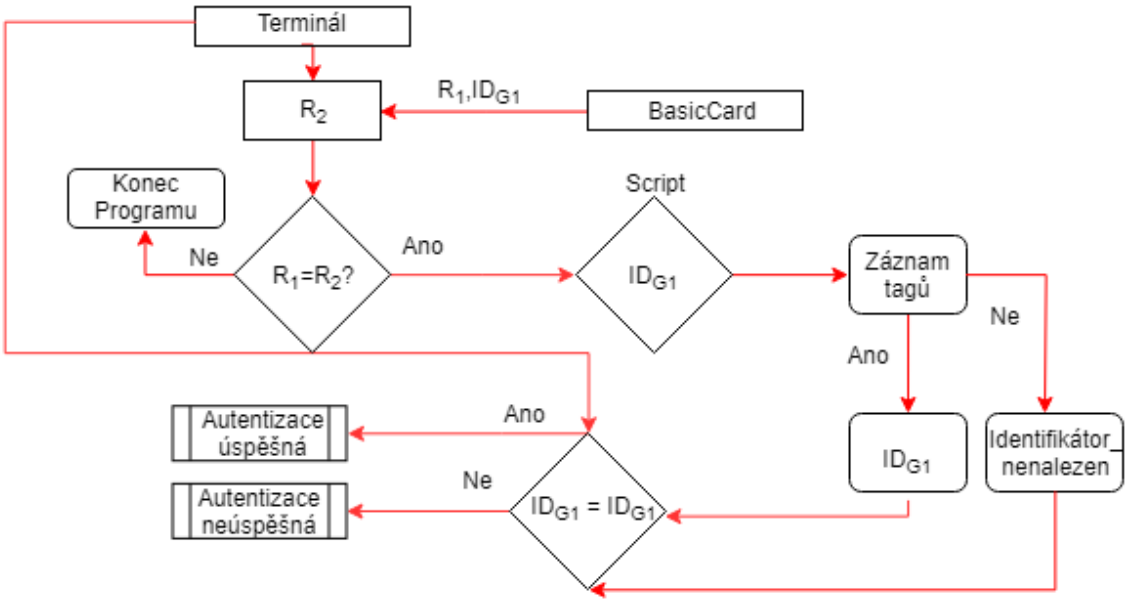
tam bylo uloženo vždy po ukončení skenování, předtím, než by čtečka začala skenovat znova a informace by byly přemazány. Při tomto pokusu bylo ale maximálně docíleno vytvoření souboru. Do souboru se už ovšem nepodařilo vykopírovat jednotlivé informace z GUI. Program má buď v sobě implementovanou ochranu proti takovému kopírování a nebo pokus selhal na základě nedostatečných znalostí s prováděním operací umožňujících takovéto čtení z jednotlivých programů, se kterými nebyla žádná zkušenost.

6.2.5 Aktuální princip předávání ID do terminálu

Provedené řešení, uskutečněné pro odevzdané softwarové řešení, využívá C sharp script. Script jako první krok detekuje předem určenou stavbu tagu, která musí mít 12 dvojic. Dvojice může být jak „ab“ tak i „2h“ nebo „22“, následně musí být mezi každým z těchto identifikátorů pomlčka. Pro detekování tagu ID musí mít tvar: 30-05-fb-63-ac-1f-13-11-ec-88-00-28.

Při rozdílném tvaru tagy nejsou detekovány a výsledek pro protokol bude neúspěšná autentizace, protože hodnota nebude odpovídat hodnotě ID_{G1} na kartě. Při takové situaci je uložena do txt souboru hláška „Identifikátor nenalezen“.

Tagy, které byly zapůjčené, mají již zmíněný tvar a při podmínce, že ID_{G1} má 64 bitovou délku, je na kartě nastavena pouze hodnota „88-00-29“. Script detekuje veškeré záznamy v txt souboru s názvem „VysledkyCtecky.txt“ a při nalezení shody pro definovaný tag, který má nastaven, uloží do textového souboru pouze hledanou hodnotu.



Obr. 6.6: Blokové schéma principu předávaní ID.

Soubor je následně načten terminálovým programem. Hodnota ID_{G1} je vyjmuta z R zprávy, která byla poslána přes zabezpečenou komunikaci pomocí AES 256 bit. Po získání hodnoty ze souboru si musí hodnota ID_{G1} z karty a hodnota z textového souboru odpovídat, aby terminál vygeneroval zvuk, který je signálem pro úspěšnou autorizaci.

Komunikace mezi čtečkou a terminálem je tedy statická, tvořená přes určitý textový soubor. Tagy se musí nejprve vložit do tohoto textového souboru a následně může být spuštěn vyhodnovací script, zda je v souboru uložen požadovaný prvek odpovídající identifikátoru na kartě.

Výpis 6.1: Aplikovaný Script

```
var rgxMatch = Regex.Matches(test, "\\w{2}-\\w{2}-\\w{2}-
\\w{2}-\\w{2}-\\w{2}-\\w{2}-\\w{2}-\\w{2}-\\w{2}-\\w{2}-
\\w{2}");
  foreach (Match mtch in rgxMatch) {
    txtBuffer += txtBuffer + mtch+ ",";
    if (mtch.Value.Contains("88-00-29"))
    tagBuffer = mtch.Value;
            }
if (tagBuffer != String.Empty)
{
Console.WriteLine("Uzivatel_vlastni_pozadovany_prvek");
   tagBuffer = "88-00-29";
}
 else {
    "Uzivatel_nema_pozadovany_prvek"'
    tagBuffer = "Identifikator_Nenalezen";
}
```

Ve výpisu kódu 6.1 můžeme vidět hlavní části scriptu, který zajišťuje funkci popsanou v 6.2.5.

7 Závěr

V první polovině bakalářské práce byla zpracována autentizace pomocí RFID prvků a problémy, které mohou nastat a které se vyskytují kolem RFID technologie. Začátek práce popisuje aktivní a pasivní RFID prvky a rozdíly mezi nimi. Dále jsou představeny systémy a jejich principy pro rozhodnutí, jaký typ systému je vhodný do určitých oblastí potřebných RFID technologii.

V kapitole (5) bylo provedeno měření tagů, u kterého limitujícím prvkem byla čtečka Roger AS 399x omezující dosah na 5 m pro pasivní tagy. Rychlost čtení splňovala podmínku úspěšného přečtení tagu do 6 ms na různé vzdálenosti. Tato podmínka byla stanovena výrobcem RFID UHF antény. Byly měřeny parametry jako jsou vzdálenost úspěšného přečtení, chybovost, reakční doba, než je tag čtečkou zpracován a úspěšně považován za přečtený.

Druhá polovina bakalářské práce je zaměřena na implementaci autentizačního protokolu navrženém na ústavu VUT v Brně. Protokol je zaměřen na čipové karty s procesorem schopným počítat jednotlivé matematické a kryptografické operace. Příkladem takové operace je násobení bodu na eliptických křivkách a nebo možnost generovat parametr jako je tajný sdilený klíč. Pro implementaci byla zvolena platforma BasicCard a zdrojový kód byl psán v jazyku Basic.

Původní protokol zde byl upraven, jelikož zde nebyla implementováno čtení z databáze, v níž by se vyčítaly ID tagů pro jednotlivé skupiny. Realizované programy odpovídají schématům „Terminál jako ověřovatel“ a „Karta jako ověřovatel“. Byla porovnána časová náročnost pro jednotlivé operace, aby protokol proběhl úspěšně. Současně bylo zaznamenáno, jak velký časový rozdíl byl, když se celá implementace simulovala pouze v terminálu. Následně případ, kdy byla využita reálná karta v kombinaci s terminálem, který představoval PC.

Literatura

[1] John Wiley Sons,2010 *RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication*

[2] JUELS, Ari *RFID security and privacy: A research survey. IEEE journal on selected areas in communications, 2006, 24.2: 381-394*

[3] XIE, Wei, Lei XIE, Chen ZHANG, Quan ZHANG a Chaojing TANG *Cloud-based RFID authentication. Cloud-based RFID authentication. 2013.* Dostupné z URL: <https://ieeexplore.ieee.org/document/6548151>

[4] TURCU, Cristina, Remus PRODAN, Marius CERLINCA, Tudor CERLINCA a Cornel TURCU *Information Storage on RFID Tags: Some Structural Optimizing Solutions* 5. I.2007, 2007(9776979) [online]. Dostupné z URL: <https://ieeexplore.ieee.org/document/4368123>

[5] Dostupné z URL: *How to Select a Correct Tag – Frequency. Rfid4u [online]. [cit. 2018-11-13].* <https://rfid4u.com/rfid-basics-resources/how-to-select-a-correct-tag-frequency/>

[6] Bořutík Stanislav *Bezpečnost technologie RFID*, Vysoké učení technické v Brně. Fakulta informačních technologií ; 2013. <https://dspace.vutbr.cz/xmlui/handle/11012/52700>

[7] Rahman, F, Hoque,ME, Ahamed, Si *AnonPri: A secure anonymous private authentication protocol for RFID systems 2017 , ISSN 0020-0255.* <https://www-sciencedirect-com.ezproxy.lib.vutbr.cz/science/article/pii/S0020025516305199>

[8] CHIH HUANG, Yu *Secure Access Control Scheme of RFID System Application. Secure Access Control Scheme of RFID System Application.* 2009, 2009(10908612), 4. DOI: 10.1109/IAS.2009.223, <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5283855>

[9] BURDA, K In *Autentizační kryptosystémy*, Sdělovací technika, 2016, roč. 64, č. 12, s. 31-33. ISSN: 0036-9942,

[10] TAGRA, Deepak, Musfiq RAHMAN a Srinivas SAMPALLI *Technique for preventing DoS attacks on RFID systems.* Croatia, 2010, 2010(11637601), 5., <https://primo.lib.vutbr.cz/primo-explore/fulldisplay?docid=TN_springer_s0-387-23462-4_108244_Chap15&context=PC&vid=420BUT&search_scope=Everything&tab=default_tab&lang=cs_CZ>

[11] S.A. Weis, S.E. Sarma, R.L. Rivest, D.W. Engels *Security and privacy aspects of low-cost radio frequency identification systems"*,Security in Pervasive Computing, Lecture Notes in Computer Science, 2004, Springer-Verlag, LNCS no. 2802, pp. 201–212.,

[12] SPIEKERMANN, Sarah, Oliver BERTHOLD, Philip ROBINSON, Harald VOGT a Waleed WAGEALLA *Maintaining Privacy in RFID Enabled Environments. Privacy, Security and Trust within the Context of Pervasive Computing*. Boston, MA: Springer US, 2005, 780, s. 137-146. DOI: 10.1007/0-387-23462. ISBN 9780387234618. <https://primo.lib.vutbr.cz/primo-explore/fulldisplay?docid=TN_springer_s0-387-23462-4_108244_Chap15&context=PC&vid=420BUT&search_scope=Everything&tab=default_tab&lang=cs_CZ>

[13] Landaluce, H., Perallos, A., Angulo *Managing the number of tag bits transmitted in a bit-tracking RFID collision resolution protocol* Sensors, 14(1), 1010-1027. doi:http://dx.doi.org/10.3390/s140101010, <http://dx.doi.org/10.3390/s140101010>

[14] BURDA, Karel *Základy elektronických zabezpečovacích systémů*, Purkyňova 95a, 612 00 Brno, www.cerm.cz: LITERA BRNO, 2017. ISBN 978-80-7204-967-7.

[15] MOHAMMED, Usama S. a Mostafa SALAH *Tag Anti-collision Algorithm for RFID Systems with Minimum Overhead Information in the Identification Process*. Radioengineering [online]. Společnost pro radioelektronické inženýrství, 20(1), 61-68 [cit. 2018-10-29]. ISSN 1210-2512. <https://dspace.vutbr.cz/xmlui/bitstream/handle/11012/56799/11_01_061_068.pdf?sequence=1&isAllowed=y>

[16] MITROKOTSA, Aikaterini, Melanie R. RIEBACK a Andrew S. TANENBAUM *Classification of RFID Attacks* <http://visionlab.tudelft.nl/sites/default/files/IWRT08.pdf>

[17] LEI ZHU, Tak-Shing Peter a Tak-Shing Peter YUM *The Optimal Reading Strategy for EPC Gen-2 RFID Anti-Collision Systems. Communications* <https://primo.lib.vutbr.cz/primo-explore/fulldisplay?docid=TN_ieee10.1109/TCOMM.2010.080310.090421&context=PC&vid=420BUT&search_scope=Everything&tab=default_tab&lang=cs_CZ>

[18] UYSAL, Ismail a Nikita KHANNA *Q-frame-collision-counter:* A novel and dynamic approach to RFID Gen 2's Q algorithm. In: RFID Technology and Applications (RFID-TA) <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7379805>

[19] *Active and Passive* [online] RFID4u [cit. 2018-11-13]. <https://rfid4u.com/rfid-basics-resources/how-to-select-a-correct-rfid-tag-passive-vs-active/>

[20] *Autentizace Entit* ČSN ISO/IEC 9798-5. 2001. Praha: Český normalizační institut, 2001, 44 s.

[21] *Cíle a metody kryptografie* [online]. [cit. 2018-11-28] <https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=7021;lang=en>

Seznam symbolů, veličin a zkratek

RFID	Radio frekvenční systém identifikace – Radio Frequency Identification
EPC	Elektronický identifikační kód – Electronic Product Code
DB	Databáze
TDMA	Časový interval pro přístup k médiu – Time Division Multiple Access
SDMA	Prostorový interval pro přístup k médiu – Space Division Multiple Access
FDMA	Frekvenční interval pro přístup k médiu – Frequency Division Multiple Access
ACK	Potvrzující paket – acknowledgement
TID	Identifikační čislo – Tag Identifier, každý tag ma unikátní TID
CPC	Centální počítač – Central Computer
DOS	Odmítnutí služby – Denial of services
A	Entita která vyžaduje přístup
B	Ověřující entita
EKV	Elektronická kontrola vstupu
$\boldsymbol{K_x}$	Tajný společný klíč
$\boldsymbol{K_m}$	Master klíč použitý pro výměnu dat mezi entitami
LF	Nízké frekvence – Low Frequency
HF	Vysoké frekvence – High Frequency
UHF	Velmi vysoké frekvence – Ultra High Frequency
r	Náhodné číslo – Random number
$\boldsymbol{W}$	*Svědek*
$\boldsymbol{d}$	*Výzva*
$\boldsymbol{D}$	*Odpověď*
$\boldsymbol{V_k}$	*Veřejný klíč*
$\boldsymbol{S_k}$	*Soukromý klíč*
h	Hashovací funkce
RTF	Čtečka mluví první – Reader Talk first
ms	Mili sekundy
$\mathbf{ID_{G1}}$	Identifikátor pro skupinu
$\mathbf{R_1}$	Zpráva pro porovnání k autentizaci (terminál)
$\mathbf{R_2}$	Zpráva pro porovnání k autentizaci (karta)

Seznam příloh

A Obsah přiloženého DVD

Na DVD jsou přiloženy adresáře s názvem:

- Karta jako ověřovatel
- Terminál jako ověřovatel
  V těchto dvou adresářích najdeme aplikace, které stačí importovat na platformě BasicCard. Aplikace realizují autentizační protokol. Návod jak importovat a spustit programy je umístěn v souboru readme.txt.

Spolu s adresáři jsou zde umístěny soubory:

- readme.txt – Slouží jako návod jak importovat a spustit aplikace. Popisuje nastavení pro virtuální nebo realný hardware.
- ScriptProtokolu – Zkompilovaný zdrojový kód scriptu. Při spuštění se nám vytvoří příslušný adresář, který popisuje zda v záznamu tagů. Při spuštění na jiném PC je třeba upravit zdrojový kód, vše popsané v readme.txt.
- ZdrojovyKodScript – Soubor typu CS. Kompletní zdrojový kód pro script.

Poslední soubor na DVD je PDF soubor. Tento soubor je záznam Bakalářské práce v elektronické podobě.